The Mobile Subscriber Equipment (MSE) Telecommunications Functional Model

United States Army Signal Center

Fort Gordon, Georgia

Leader College of Information Technology (LCIT)

Functional Area 24
Telecommunications Systems Engineer Course
Class 05-01

Final Thesis

28 September 2001

MAJ Eric Blair
MAJ Reggie Morgan
CPT Mark Mattei
CPT Hubert Wagstaff
CPT Bryon Hartzog

The Mobile Subscriber Equipment (MSE) Telecommunications Functional Model

THESIS

With commercial-off-the-shelf (COTS) technologies and equipment becoming more widely utilized within military applications, Army communicators must have an in depth knowledge of telecommunications systems in order to quickly and accurately understand how legacy and future systems can be connected and interoperate. Legacy equipment is defined as everything that is being used at the present time. Realists agree that it will be a very long time before these systems are completely replaced. As Army communications systems transform and become more COTS-based, the requirement to interconnect with legacy systems will continue. Commercial communications systems are commonly described using telecommunications functional or component models. Future Army communicators will use models to engineer, monitor, validate and restore Army, Joint, and commercial telecommunications systems and interconnect these systems when required. This is a record of our research effort to present the Wire Subscriber Access (WSA) area of the Mobile Subscriber Equipment (MSE) using a layered, functional model.

1. Background

The purpose of any model is to be able to focus on certain aspects or functions without being overwhelmed by details. A model is an abstraction of a system where the details outside the proposed area are made invisible but not ignored.[1] The International Telecommunications Union-Telecommunications Sector (ITU-T) X.200[2] recommendation specifically provides a base for the Open Systems Interconnect (OSI) model referenced by communications architectures. All telecommunication systems do not follow this particular model, but it is widely accepted and used among commercial telecommunications engineers.

The OSI Reference Model consists of functions grouped into layers and can be viewed as an ordered set of subsystems, with a security and management plane running down the side and back respectively. Each higher layer requests services from the layer below. End user applications request service from the Application Layer, which in turn requests service from the presentation Layer followed by the Session Layer. Below the Session Layer are the Transport, Network, Data-link and the Physical Layer. The Physical Layer formats and provides the interface onto some form of physical transport medium.

Modeling a telecommunication interconnection system may or may not use the same set of functions grouped in the same layers. A telecommunications model is a framework for interconnection of end user entities and provides a description of how services, such as voice or data, are accessed, transported, switched, controlled, secured and managed, through the layers up to the end user application. Whether, the model is as simple as access, transport, and switching systems or as detailed as the OSI reference model, the goal of the model is to sort out what is happening and where.

The Army's Mobile Subscriber Equipment is the Army's "Echelons Corps and Below" (ECB)[a] telecommunications system. The MSE architecture forms a grid of systems capabilities throughout the Army corps area. The network consists of Node Center Switches (NCS)[b], Radio Access Units (RAU)[c], Large Extension Nodes (LEN)[d] and Small Extension Nodes (SEN)[e]. Node Centers provide the backbone of the network, while LEN's and SEN's provide wire subscriber access and RAU's provide mobile radio access. MSE was developed from a French system and designed and fielded in the late 1980's and early 1990's. The circuit switch network was upgraded with a packet switch network overlay added in order to provide data services to the subscribers.[3]

2. Goal

This research is part of a larger effort to map the entire Area Common User System (ACUS)[f] to a usable, layered, functional, telecommunications model. The purpose of this project is to provide future Army communicators a tool to help them engineer, monitor, validate and restore Army, Joint, and commercial telecommunications systems and interconnect these systems when required. In the process of mapping a known, legacy communications system to the model, we

[a] Echelons Corps and Below (ECB) refers to the units in a standard tactical Army Corps

[b] Node Center Switch (NCS) is the Army's tactical backbone tandem, Flood Search Routing mobile tactical telecommunications switching system.

[c] Radio Access Unit (RAU) is the Army's tactical mobile voice subscriber interface.

[d] Large Extension Node (LEN) is the Army's large mobile voice and data wire subscriber node

[e] Small Extension Node (SEN) is the Army's small mobile voice and data wire subscriber node.

[f] Area Common User System (ACUS) is the Army's current set of tactical telecommunications equipment. It includes Mobile Subscriber Equipment, Digital Group Multiplexing equipment as well as single channel FM, HF and satellite systems

have reinforced our own proficiency with respect to modeling telecommunications systems as well as with respect to the MSE system. This is a lesson, which may be used to develop a way to better educate communicators about future and legacy communications systems. Our approach was to develop a layered model to illustrate the protocols or functions used, where they were used, and how they interrelate with other protocols or functions. Using the OSI Reference Model as an example we organize the functions, services and protocols provided by each layer or plane. The User-to-Network (UNI)[a] model depicts the protocols, services and functions of the user accessing the network. The UNI model does not describe the signal flow through the network, but describes the possible user interface requirements to access the network. The Network-to-Network (NNI)[b] model depicts the functions, services and protocols used within and between the subnetwork. Again, this model does not show the signal flow through the network, rather it shows the network interface requirements within the subnetwork.

3. Scope

The focus of our research began with the user, control, management, and security protocols of the Wire Subscriber Access area, which is one of the five functional areas of the MSE system, as defined by The "MSE System Specification."[4] However, we expanded the scope to include the MSE Network-to-Network and user voice and data to-Network interfaces. The User-to-Network Interface (UNI) is defined as an abstract reference point between a user device and the circuit and/or packet switched subnetworks. The Network-to-Network Interface (NNI) is likewise defined as an abstract reference point between the circuit and packet switched subnetwork nodes. This did not cover all of the the MSE Transport sub-systems, the Tactical High Speed Data Network (THSDN), or ATM and FM interconnections.

4. An Overview of MSE

In order to fully understand the system, a reference model describing the UNI interface and a reference model describing the Network-to-Network Interface NNI will be used. (See Appendix A, Figure 4.1a and 4.1b). The User-to-Network interface is the interface between the end user

[a] User-to-Network Interface (UNI) is a term used to describe the interface between the end user equipment and the subnetwork

[b] Network-to-Network Interface (NNI) is a term used to describe the Network interface between subnetwork interconnections

and the subnetwork, such as a Digital Non-secure Voice Terminal (DNVT)[a] to a SEN. The NNI is between subnetwork nodes, such as between two Node Centers or between a Node Center and a SEN. (See Appendix A, Figure 1.5) Each reference model describes the functions and services associated with user and network interconnections and can be broken down into the User Plane, the Control Plane, the Security Plane and the Management Plane. The User Plane contains the functions and interactions that are occurring to the user information from the user device to network. The Control Plane contains the functions and interactions that are happening to setup, control, supervise and disconnect the user plane functions.

The User and Control Planes can further be broken down into functional layers, much like the OSI Layers. With Layer 1 of the UNI and NNI resembling the Physical Layer of OSI, Layer 2 resembling the OSI Data Link Layer, and Layer 3 resembling the OSI Network Layer.

The Security Plane contains all services and functions associated with User and Network Security and the interactions with associated planes and layers within model. The Management Plane contains all services and functions of layer, plane, system and application management. [5]

5. MSE Circuit Switched Network

The MSE Network can be broken down into two separate networks. The MSE system was originally just a circuit switched voice network, which was then upgraded to incorporate a data packet switched network. The engineering of this addition lead to the packet switched network utilizing the circuit switched network to provide trunking between PS nodes. Although, the circuit switched network provides a transport system for the packet switched network, it does not switch the packet traffic. As information is past into the packet switched network, it is then routed through the circuit switched transport network to another packet switch. The NNI's and UNI's for the packet switched network are separate entities and can be broken in to separate planes allowing for further abstraction.

5.1 User and Control Plane's of the User-to-Network Interface (UNI)

5.1.1 Model Orientation

The User Plane of the Circuit Switched Network describes the protocol interactions and signal flow associated with digital and analog telephony and data device interfaces within the UNI. The

[a] Digital Non-secure Voice Terminal (DNVT) is a voice to digital converter user end terminal.

control plane contains the interactions for signaling control and supervision during a subscriber's request for service. The service being provided by the user plane is user-to-user, secure and non-secure voice, and data service.

5.1.2 MSE Functional Description

Layer 1, the Physical Layer, of the User Plane and Control Plane defines the mechanical, electrical, functional and procedural characteristics for of an end user device, whether via a Digital Non-secure Voice Terminal (DNVT), Digital Secure Voice Terminal (DSVT), Mobile Subscriber Radio Terminal (MSRT), analog telephone, computer or fax. (See Appendix B, Figure B2)

The mechanical user interface characteristics are basically WF-16, copper and steel wires from the binding post on the DNVT or DSVT to the push plugs on the junction box, J-1077. The connection from the J-1077 then follows a 26-pair cable to the signal entry panel of the SEN, which provides network interface, and is terminated in the SB-4303, switchboard, on a Diphase Loop Modem A (DLPMA) card. The radio terminal RT-1539 or ER-222 for the MSRT terminates the 4-wire connection from the DSVT with a special purpose cable. Analog connections are made using two wire connections from the Dial Central Office (DCO) into the signal entry panel through line terminating unit (LTU), which provides a four-wire interface connection to the SEN to a Type 5 card. Data devices such as the AN/UGC-137A (V) 2 computer or AN/UXC-7, fax, will access the network through the DNVT or DSVT using a single 55 pin connector type MS27468T17B35P (mating connector MS27467T17B35S). The pin out for this connector is shown in Appendix B, Table B1.

The electrical signal transmitted between the user and the network interface is a 3-volt, peak-to-peak, 16kbs, condition diphase balanced (CDP) waveform described in electrical specification in Appendix B, Figure B1. This is also the same signal transmitted from the ER-222 for the MSRT to the RAU.

The functional operation of the telephone is to provide the user with a full duplex circuit. This circuit is procedurally accomplished by connecting the two green wires of WF-16 to the transmit binding-post on the phone and the two brown wires to the receive binding-post and connecting the distant end to the top and bottom quadrant on the J-1077 respectively.

Layer 2, the Data Link Layer, defines the framing format for control information and user data sent across network interface. The specific framing format of this layer is not specified.

Layer 3, the UNI Network Layer, defines circuit routing control. This is accomplished using an eight bit cyclically permutable codeword (Appendix B, Table B2-B4) that represents supervisory information such as a SEIZE for service, ringing, acknowledgments, and special call handling features sent between the telephone and the network and between network interfaces. The ER-222 (RT-1539), generates some of these messages as tones shown in Appendix B, Table B5, B6. The transmissions of these codewords are sent as a continuous bit stream between the network access nodes and the switch until timed out if not acknowledge. The codewords from the DNVT are sent for ten seconds before timing out without an acknowledgment. Codewords from the DSVT vary based on the codeword, either continuous until time-out or up to 256 times (Appendix B, Table B7, B8), and 1024 times from the ER-222 to the NCS. A digital scanner monitoring the line for the Digital Signal Generator (DSG), which generates all codewords and digitized tones, interprets these codewords. A procedural sample of the codeword exchange for disaffiliation is described in Appendix B, Figure B3. The user' s voice is converted to a digital bit stream by the Continuously Variable Sloped Delta (CVSD) modulator in the digital telephones and converted in the LTU for analog subscribers at a higher layer outside of the model.

5.2 User and Control Planes of the Network-to-Network Interface (NNI) (Circuit Switched Network):

5.2.1 Model orientation

The User plane of the NNI describes the interactions of user information as it flows through the network. In a circuit switched network the interaction for call set-up, control and signaling happens before the circuit is in place. Once the information is ready to be sent, a physical circuit has already been established, and ready to have traffic flow over it. The User Plane of the NNI has only a "pass through" function at Layer 3. All of the interactions (encoding, multiplexing, framing) happen at Layers 1 and 2. Information is sent from a device to a switch, the route through the switching matrix is already a physical circuit and there is no need for any user plane Network Layer interactions.

The control plane of the NNI circuit switched network within the MSE system is to provide signaling, supervision, routing, and switching of circuit switched channels. As a Layer 3 control or supervision message moves into Layer 2, it must first enter an upper Layer 2 sub-layer, and then be passed down to the lower sub-layer 2 for multiplexing and channelization. All interactions in the Control Plane occur in order to set-up, control, supervise and disconnect a circuit. This plane contains the protocols necessary for sending routing, control, supervision, signaling and addressing information between switches.

5.2.2 NNI Layers 1 and 2, MSE Transport System

The Physical Layer of the OSI model has the following functions contained within it: physical connection activation and deactivation, physical-data-unit-transmission (PSDN) and Physical Management. The Physical Layer performs these functions in order to provide service the Data Link Layer. The services it provides to the Data Link include physical connections, transmission of physical service data-units, physical connection end points, circuit identification, fault notification and quality of service parameters. Although, there are numerous ways to transport signals used throughout the MSE System. The important area is to focus on is the cable interface. The Line of Sight UHF radio transmission (LOS), SHF radio transmission, and tactical Satellite (TACSAT) equipment used can be considered a transport system, only transporting Layer 1 and 2 information between identical NNI's.

In the Physical Layer, the Network-to-Network interface (Figure 2 Appendix C) consists of functional, procedural, mechanical and electrical specifications of how information is placed on a media. The signals are encoded on the line in a conditioned diphase format, much like Differential Manchester coding. The cable consists of two twisted co-axial cables. The two axils terminate in a MIL standard Cannon plug universal connector.

In the Network-to-Network Interface, the Data Link Layer places channels in time slots to form a Digital Transmission Group (Figure 9, Appendix C). All Digital Transmission Groups use a fixed length frame of 0.5ms duration at a voice digitization rate of 16 kb/s and 0.25 ms duration at a voice digitization rate of 32 kb/s. The basic frame organization common to all Multiplex Signal Formats (MSF)[a] provide time slot assignments for a primary overhead channel and additional traffic channels. The fixed length frame is defined as a major frame and is

[a] Multiplexed Signal Format (MSF) is a grouping of similar multiplexing formats using different framing and signaling positions

delineated by the positions of the framing bits. The time slot structure within the major frame is organized into either four or eight minor frames. The common signaling sub-channel assignment is used for signaling and supervision necessary to manage and control inter-switch traffic. These switches maintain a fixed relationship between this sub-channel and the traffic channels being controlled.

Digital Transmission Groups (DTG' s) are organized into four basic types, Type 1, 2, 3, and 4 and have three primary overhead channelization plans designated as Type L, Type O, and Type S. These applications dictate specific arrangements of the MSF in terms of the time slot to channel assignments. All MSF use a fixed length frame defined by a single frame time slot. The common frame plan defines the first time slot in each frame as containing the framing bit. From one frame to the next, this time slot produces the in-sync frame pattern consisting of an alternating one zero sequence at a 2/4 kb/s rate. These frame bits define the beginning of each new frame of time slots, which are associated with the individual channels.

5.2.3 NNI Layer 2 User and Control Protocols

In addition to the Layer 2 functions already described, additional framing, encoding and decoding is accomplished on a channel by channel basis. Each of the additional Layer 2 functions will be described in the respective functional area. For instance, the encoding and framing that happens to a voice circuit, is not the same as a signaling message being placed onto a Common Channel Signaling channel.

The Network Layer functions are routing and relaying, network connections, network multiplexing, segmenting and blocking, error detection, error recovery sequencing, flow control, expedited data transfer, reset, service selection, and Network Layer management. The Network Layer provides certain services or elements of services to the transport level. The network addresses, network connections, network connection endpoint identifiers, network service data unit transfer, quality of service parameters, error notification, sequencing, flow control, expedited network-service-data-unit transfer, reset, release and receipt of confirmation. [6]

The MSE NNI circuit switched control plane is broken down into user interface control and network interface control. The User interface control plane describes the signaling call control and supervision between a user device and the network switch. The Network interface control provides for signaling, call control, and supervision of calls or circuit connections, as well as the switch to switch or switch to Group logic unit of the RAU routing, affiliation, blacklisting and addressing information.

Layer 2 or the Data Link Layer of any system describes the means to activate, maintain and deactivate the Data Link. We can define the upper sub-layer of the **Layer 2 protocol as the Common Signaling Channel Protocol.** It encompasses, the encoding, decoding, storage and message formatting to allow for the signaling between the two switches. Although, these protocols are put into channels by the lower Layer 2 functions, they are commonly referred to as channel names; the Trunk Signaling Buffer channel (TSB), The Digital-In-band-Trunk-Signaling (DIBTS) channel and the NATO Signaling Channel. For Detailed information on the Common Channel Signaling protocols, see Appendix D.

5.2.3.1 NNI Layer 3 Protocol (Flood Search Routing Protocol)

Layer 3 provides routing and relaying of network connections. Additionally, it provides for the transfer of information between end systems across some sort of communications network. The Network Layer provides certain services or elements of services to the higher layers, relieving them of the responsibility or knowledge of any transmission or switching technologies used to connect systems. The services provided from Layer 2 to the Network Layer are the request for service messages, precedence level, security requirements, and mode data or voice. Once the message is received the local routing tables are checked and the Flood Search Protocol determines the route. The **Flood Search Routing Protocol** sends a message to all connected switches asking for service. If the service cannot be provided, the number is not at affiliated off that switch, the request is forwarded to from that switch until it is found once the number or service can be provided the parent switch or switch that can provide the service determines the best route to the caller asking for service and sets up the call. Detailed information is defined and is contained in ICD-13 and ICD 14[a]. See appendix D for detail on signaling messages and process.

5.2.3.2 RSS Signaling Protocol

At Layer 1 and 2, the routing and switching updates use the Routing Sub-System (RSS) signaling channel between switches. This RSS channel provides for the communication between the

[a] ICD-13 and 14 are GTE Interface Control Documents, which describe the control and signaling. Common Channel Signaling, Flood Search Routing and Digital In-band Signal documents are proprietary to GTE, as specified in the Army Contract and can not be obtained

Routing subsystems. This involves transfer of routing table information, user affiliation and black listing information. The details of this channel and the Layer 2 protocol were specified within ICD-13 and ICD 14. See appendix D for details on signaling and messages.

5.2.3.3 GLU Signaling Protocol

The last control and signaling channel is the Group Logic Unit (GLU) Channel. The GLU is a signaling processing device, which enables radio transmission access control. The channel is used for frequency updates either from the System Control Center (SCC) to the GLU or to subscribers from the GLU. The Layer 3 of the GLU signaling protocol contains the information necessary for transfer from the node center to the GLU. The Layer 2 of this protocol contains the messages necessary for carrying this information across the GLU channel. Detailed information on the Layer2 and Layer 3 messages could not be found. . See appendix D for details.

6. User and Control Plane of the packet switched UNI and NNI (MSE Packet Switching Network - MPN)

The tactical packet network (TPN) allows users to transmit data across the boundaries of the tactical network. The packet network can span across at Echelons Corps and below (ECB), which is referred to as the MPN, and Echelons Above Corps (EAC), which is referred to as TRI-TAC packet overlay. The TPN performs this function similar to circuit switching; however, it fragments the traffic into small packets, attaches the destination address and routes each packet to its intended destination through the network via the quickest available path known. The MPN switching network equipment (See Figure 4.3.1, Appendix E) consists of a Packet Switch (PS) (AN/TYC-20V), which provides users access to the MPN and routes data packets through the MPN; a gateway router (AN/TYC-19), which interconnects MPNs to other MPNs or to another types of LAN/WANs such as the Internet, MILNET and DDN[a]; signal data converter (CV-4206/TTC) which converts the users data terminal equipment (DTE) digital signals to a 16kbps conditioned diphase (CDP) signal; and other signal converters (MSE Data Interface Device (MDID) and Tactical Terminal Adapter (TTA)), which allow data users to interface with the MSE circuit switch. The MPN is a Wide Area Network (WAN), which uses DDN Standard

[a] DDN is the Defense Data Network, which uses the TCP/IP protocol suite for layers 3 and higher

X.25, an ITU-T Standard Protocol, which defines how two user hosts (DTEs) communicate across the WAN via Data Circuit-terminating Equipment (DCE).[7]

Users within the MPN have three ways to access the packet network (see Figures 4.3.2, 4.3.3 4.3.4, Appendix E).[8] They can enter thru a local LAN which is connected to the packet switch, directly through a X.25 direct connect interface on the packet switch, where the EAC switch allows 8 connections, LEN allows 7 connections and the SEN allows 5 connections, and finally thru a DNVT and DSVT via dial-up, where CDP converters, such as the MSE Data Interface Device (MDID), Tactical MSE Interface Family (TMIF) and Tactical Terminal Adapter (TTA), allows the user to emulate the DNVT/DSVT.[9] [10]

The MPN provides users two types of X.25[a] services, Standard and Basic, and directory email service provided by the Tactical Name Server (TNS) and the Mail Transfer Agent (MTA). Standard X.25 service allows for communication between X.25 DTEs and other user hosts that utilize the Department of Defense (DoD) suite of protocols. These protocols consist of Transmission Control Protocol/Internet Protocol (TCP/IP), TELNET, File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP). Basic X.25 service allows user DTE using X.25 protocols to communicate with other X.25 DTEs within the same subnetwork that do not use the DoD upper level protocols. The TNS provides an automatic affiliation process similar to that provided to voice users. It performs user registration, a means for users to determine the network location of other users if connected and host address resolution. The MTA is essentially an email component of the MPN. The MTA performs email store and forward, absent host coverage and multiple addressing.[11]

6.1 LAN Access to the MPN

For a host user to access the MPN via a LAN, it must comply with the IEEE 802.3/Ethernet 2 Standards. The LAN user can communicate with other LAN hosts on the same segment or on a different segment, which is interfaced with the MPN. The LAN user can also communicate with X.25 host users interfaced with the MPN. On local segments, Carrier Sense Multiple Access with Collision Detection (CSMA/CD) controls communication between hosts. The Integral Gateway (IGW) inside the PS provides the path for local LAN hosts to communicate with non-local LAN hosts or X.25 hosts.[12] IGW allows MPN LAN hosts to send datagrams to non-LAN hosts without

[a] X.25 is a ITU-T specification for user interface into a packet switched network. X.25 does not define the subnetwork characteristics. MSE was designed to use a modified X.25 specification for subnetwork functions.

knowledge of the TPN topology. The IGW also serves as a Reverse Address Resolution Protocol (RARP) server, by allowing LAN hosts to obtain an IP address from its connected PS and register with the Tactical Name Server (TNS), which provides directory service for MPN users.

As a LAN host sends traffic to another LAN or non-LAN host it is encapsulated in protocols associated with the seven OSI Layers. Protocols such as FTP, SMTP for email messaging and TELNET are used at Layers 7-5. At the Transport Layer 4, TCP is used to encapsulate the higher Layers providing reliable flow and error control. At Network Layer 3, TCP is encapsulated with IP, enabling the user to interconnect with other networks that are connected to the MPN. At Data Link Layer 2, IP is encapsulated with IEEE 802.3 Medium Access Control (MAC) protocol. Within a LAN environment, IP is encapsulated into the Logical Link Control (LLC) / MAC protocol; however, within the MPN X.25 NNIs, LLC is not used, because the X.25 MPN network provides call establishment, data transfer, and call termination services. Lastly, at Layer 1, the frame(s), if fragmentation is required, are converted to an electrical bit stream IAW the 10Base2 standard across Thin-LAN coax. (See Figure 4.3.7, Tab 1, Appendix E) If the traffic is destined for a non-local LAN host, the 10Base2 signal passes thru the signal entry panel (SEP) into the transceivers, where the signal is converted to the PS CDP/ 16kbps bit stream. From there the IGW provides the path to the PS, where upon the traffic enters the X.25 MPN PSN.[13] (See Figure 4.3.7, Tab 1, Appendix E)

6.2 X.25 Access to the MPN

As stated in the paragraph 4.3, X.25 host users can access the MPN two ways: 1) connecting to the PS directly or 2) via dial-up by interfacing thru the circuit switch and then getting passed into the PS. Additionally there are 2 types of X.25 service that users can obtain: Basic X.25 service and Standard X.25 service. The major difference is that standard service uses the DoD higher protocol suite, allowing the host user to interconnect to other networks besides the MPN, such as Private Data Networks (PDN) or the Defense Data Network (DDN). X.25 hosts obtain IP addresses from the PS that are connected to, by sending a Call Request packet and utilizing the NETID private facility, which is discussed in Appendix E.

Basic X.25 service host users, who do not use the DoD higher Layer protocols such as TCP/IP, encapsulate associated applications at the Network Layer 3 with X.25 Packet Layer Protocol (PLP). At the Data Link Layer 2, PLP is encapsulated with Link Access Protocol-Balanced (LAPB). Then at Layer 1, the frames are converted to the EIA-RS-432 standard for transmission over the applicable media. For the direct X.25 users who connect directly into the PS, the RS-432 signal is converted to CDP / 16Kbps by the SDC inside the PS. For the dial-up X.25 users, the RS-432 signal is converted to CDP / 16Kbps by the CDC, which emulates the DSVT or DNVT IOT access the circuit switch, where it is passed to the PS thru the PHSTI card.[14]

The Packet Switch Host Trunk Interface (PSHTI) Circuit Card Assembly (CCA)s are located in the TDSG(M)[a] nests of the NCS and the LEN. They provide the interface between the packet switch and gateway and the circuit switch. In host mode, the PSHTI has three 16 kbs channels to and from the packet switch and three 16 kbs channels to and from the matrix. This mode is used for the SEN and SCC links. In the trunk mode, PSHTI has one 64 kbs channel to and from the packet switch and four 16 kbs channels to and from the matrix. This mode is used for internodal links. The PSHTI multiplex and demultiplex the channels to and from the matrix. The MPN NNIs are connected via the circuit switched network physical paths, where the PHSTI CCAs provide the path to the CSN backplane matrix.

The X.25 Standard Service hosts use a subnetwork dependant convergence protocol (SNDCP)[15] that enables connectionless IP datagram service to be mapped into X.25 connection-oriented packet service. This protocol is the ARPANET[b] Host Interface Protocol (AHIP) / 1822, engineered by BBN Technologies.[16] [17] (See Appendix E) Additionally, when X.25 hosts are connecting to the DDN, the subnetwork uses X.121[c], which maps IP addresses into the DDN address format.[18] (See Figures 4.3.8 and 4.3.9 for X.25 Host to X.25 WAN Routing Diagrams, Tab 1, Appendix E)

The direct X.25 hosts interface with the PS via the EIA-RS-432 standard at Layer 1. The electrical bit stream is then converted to the CDP / 16Kbps by a Signal Data Converter (SDC) located inside the PS. (see Figure 4.3.1, MPN Packet Switching Equipment, Tab 1, Appendix E) Here the bit stream enters the MPN X.25 PSN. [19]

The dial-up X.25 hosts interface with the MPN thru the circuit switch network initially. The X.25 host's RS-432 interface is converted to a 4-wire CDP / 16Kbps by a CDP Converter (CDC), such as a MSE Data Interface Device (MDID)[20], Tactical MSE Interface Family (TMIF), or a Tactical Terminal Adapter (TTA). (See Figure 4.3.9, Tab 1, Appendix E) The data then

[a] The TDSG(M) is the Time Division Switching Group-Modified.
[b] ARPANET is the Advanced Research Projects Agency Network
[c] X.121 is an ITU-T Standard for mapping or converting Internet Protocol Addresses to X.25 Addresses.

travels across the circuit switch network until it enters a node that contains a PS. Here the circuit switch passes the data stream to the packet switch via the Packet Switch Host Trunk Interface (PHSTI) card. Here the data enters the PS and into the MPN X.25 PSN.

The X.25 standard allows open networks to implement variations on the X.25 protocol. MPN implements variations of the basic X.25 protocol at Layer 2 and Layer 3. MPN also offers services that are not defined by the Recommendation X.25 or dpANS X3.100 and that are not specifically reserved for X.25 subscribers, such as the following private facilities: Type of Service, Call Precedence, Community of Service, Logical Addressing, and IP NETID.[21] (See para. E.2, Appendix E)

6.3 MPN Control Plane

6.3.1 UNI and NNI Control Packets in X.25 (X.96) and X.75

Both the User to Network Interface (UNI) and Network-to-Network Interface (NNI) use X.25 packets to establish calls between the user to the Network and subnetwork to subnetwork. MPN follows the X.25 Supervisory (S), Information (I) and Unnumbered (U) frame formats outlined in the ITU-T X.25 standard. When the MPN local network must establish connection with an external or intra-corps network, it uses X.75. X.75 is identical to X.25, except at Layer 3, where X.75 has an additional variable length field for network utilities prior to the variable length field for facilities.[22] For the NNI, the MPN uses X.25 Call Process Signals (Cause Codes) from X.96, which was released in 1986 by the CCITT.[23] [24]

Once a user gains access into the X.25 MPN, its data packets must travel across the existing CSN paths. The PS determines the best path thru the use of one of the routing and relaying protocols. This best path is mapped to a particular port existing the PS. The packets enter the CSN by traveling thru the PHTSI CCA and into the CS backplane matrix. Upon enter the backplane, the 4 PSN trunks are Multiplexed together with that communication nodes voice channels. After the Multiplexing, the communications node must establish a virtual circuit with neighboring nodes through a call establishment. Figures 4.3.7 – 4.3.12, in Tab 1 of Appendix E portray how the PSN rides over the existing CSN.

6.3.2 Internal and External Network Routing Protocols

In order for the TYC-19 gateways to communicate with each other or existing networks, they must know what devices and networks are adjacently connected. This is accomplished by the use of routing / switching tables, which are generated and updated thru routing and relaying functions. MPN uses BBN Shortest Path Algorithm (SPF) for internal network routing and EGP and BGP-4 for external network routing. External and non-MPN routers can connect to the MPN via X.25 call establishment requests or by using the Point-to-Point Protocol (PPP).[25]

6.4 TNS and MTA Services and Functions

The TNS and the MTA are combined on a single workstation in the NCSs and TTC-39Ds nodes. The main purpose of the TNS is to provide automatic affiliation process similar to that of a voice subscriber, when they affiliate their MSE phone. TPN also performs host address resolution, user registration and provides a means for users to determine the current network location of other users on the network. In order for the LAN and X.25 hosts to register with the TNS, it must obtain its IP address. X.25 hosts can obtain their IP address from the PS their connected to by sending a call request and using the NETID private facility. LAN hosts obtain their IP address from the IGW, located within the PS.

The TNS is essentially a Domain Name Server (DNS) with automatic registration capability for the MPN. It is highly recommended to connect the TNS to an empty LAN segment that is connected to LAN port 0 on the IGW. Once a host obtains its IP address, is submits a message to the TNS using one of its default NETIDs, 192.111 or 193.111. The TNS signaling message is transmitted using the User Datagram Protocol (UDP) Layer 4 protocol. Once a host is registered, it can register is associated mailbox (MB) if authorized one. The registration process is like the host registration process, involving a request message sent to the TNS physical IP NETID.[26]

Other TNS functions include TNS Refresh used to inform the TNS that the user is still available at its current IP address, and TNS Query, which is essentially a network directory service where the host can send query messages to the TNS for information about a registered host, registered MB or another TNS.

The MTA is essentially an Email server, which performs store and forward and absent host messaging up to a maximum of 12 hours awaiting the intended user to re-register with the MPN. The MTA uses the Simple Mail Transfer Protocol (SMTP) to control messaging across the network.[27]

7 Security Plane

7.1 Model Orientation. The security plane encompasses the wishes of the sender to be assured that only the intended receiver actually receives the data and the receiver of data wishes to be assured that the received data have not been altered in transit and that the data actually came from the purported sender. Additionally, the security plane secures the network from unauthorized monitoring and the need to secure end-user-to-end-user traffic using authentication and encryption mechanisms.

7.2 MSE Orientation

A prime design consideration in development of the MSE system was to provide a means to ensure all voice and data transmissions would be secure. MSE system threats are categorized as passive or active in accordance with the strategies commonly employed. Passive threats are characterized by the actions of an intruder directed toward examination of the flow of traffic on voice and Data Links. Active threats are characterized by an intruder or authorized user accessing the transmission and modifying, deleting, delaying, duplicating, reordering, or playback of the traffic. The MSE system is designed as a secret high system. Under current design, the threat cannot access or examine the voice or data traffic traveling across MSE links. The link is secure because of a combination of physical security and cryptographic security. The focus of this research is on the cryptographic security.

7.3 MSE Functional Description

MSE is an approved network in which the Trunk Encryption Devices (TEDs), KG-94As, provide security protection at the SECRET level of all Line-Of-Sight links. The Radio Access Unit (RAU) to Mobile Subscriber Radio-telephone Terminal (MSRT) links are protected by Digital Subscriber Voice Terminal (DSVT), KY-68, Loop Key Generator (LKG) encryption for communications traffic and by the Mobile COMSEC Unit (MCU) for signaling. An approved-loop-to-approved-loop call placed through a Protected Wire Distribution Site (PWDS) of an operation center is provided secure communications. Communications between PWDSs through Node Center (NC) switches are secured by KG-94As. DSVT-to-DSVT calls are end-to-end encrypted. Direct MSRT-to-MSRT calls can be allowed in exceptional situations. DSVT-to-approved loop or approved loop-to-DSVT calls require the use of an LKG for the duration of the call. Engineering Orderwire (EOW) or Digital Voice Orderwire (DVOW) traffic is limited to communications engineering traffic (i.e. position, frequency). Call security is provided by the Node Center Switch (see appendix F)

Overall cryptographic security is a result of netted protection in four functional areas: Trunk security, Orderwire security, Switch security and Subscriber security. Procedures reflecting how the security (COMSEC implementation) is done in these four areas will be the scope of this brief. A list of equipment, by assemblage, is provided in table F-1.

7.4 Trunk Security

Trunk Encryption Devices (TEDs, KG-194As) are used throughout the system to encrypt Digital Transmission Groups (DTGs) for transmission between switches. For detailed explanation of keys see Appendix F.

7.5 Orderwire Security

VINSON (KY-57s) provide secure, half-duplex communications for orderwire over radio and cable links. Additionally, 'Over-The-Air-Rekey' (OTAR) capability is provided to MSE assemblages. For detailed explanation of keys see Appendix F.

7.6 Switch Security

The Automatic Key Distribution Center (AKDC, KGX-93A) provides for the generation, storage, and transfer of COMSEC Keys. Dual Loop Key Generators (DLKGs, KG-112s) are used to provide secure communications between MSRTs and NC/LENs and key transfers between NC/LENs. For detailed explanation of keys see Appendix F.

7.7 Subscriber Security

Cryptographic protection for wire line subscribers using DNVTs (Digital Non-secure Voice Terminals) is provided via the Trunk Encryption Device. Additional protection is provided for Mobile Subscriber Radio-Telephone (MSRTs) by using RT-1539A radios to secure the radio link with the Radio Access Unit (RAU), and a Digital Subscriber Voice Terminal (DSVT) KY-68 to secure the connection to another DSVT or to the NC/LENs Dual LKG for connection to a DNVT. For detailed explanation of keys see Appendix F.

8. The Management Plane

8.1 Management Overview

In order to understand the management plane, we must first understand what happens in the management plane. The International Organization for Standardization and ITU-T has defined the key, but not all, functional areas of Network management. Fault Management, Accounting Management, Configuration Management, Performance Management and Security Management

(FCAPS). [28] Within the telecommunications systems functional diagram, the management plane encompasses how the communications process of management is done.

8.2 MSE Management

MSE uses **Integrated Management System (IMS) software** as its application software. The IMS software provides specialized data base structure to support the Network management functions. Since management is the facilities to enable Network management and not systems management, the IMS does not do any management it self. IMS uses ICMP, SNMP, and some type of remote procedure calls (RPC) to provide displays or reports. No exact information describing the RPC' s was obtained. Within the IMS software a procedure to connect software applications is some how completed. No detailed specifications of this could be found, but because this is done using the software, and not a management protocol or framework, there must be some type of RPC to enable the interaction between the Network management central's software and the devices. How IMS actually does the management interactions with respect to the telecommunications model is the key to the management Plane of MSE.

8.3 Fault Management

Breaking down the functional areas, MSE does fault management or fault monitoring, using ICMP, SNMP and RPC' s. The requirement for fault monitoring is the system must be able to detect and report faults. Within the MSE system Fault monitoring is done using the packet switched network. There are no management facilities to receive information on any of the circuit switched systems. Knowing there is a Layer one (or circuit network link) entity with faults is a result of the packet switched network management functions. Within the packet switched system. The Manager or Network Management Central (NMC) uses ICMP and SNMP (v1) with MIB (1) agents. The Agents are located in the packet switch modem, the MSE Data Interface Device (MDID) or in a SNMP, MIB 1 agent compatible Host. IMS calls these High priority hosts due to a limiting factor in the software, which limits the number of hosts it can keep track of. Using ICMP the system is able to check for connectivity or destination unreachable, end to end delay, as well as end-to-end loss percentages. For details on ICMP and SNMPv1 with MIB 1 see Appendix H.

8.4 Accounting Management

Accounting management is a facility that keeps track of accounting information of managed objects. For a typical system, this may be charges related for use of a service on that managed object. Within the MSE or IMS systems no software specific accounting management has been adopted. If a host has an agent that supports MIB 1, and that host was providing a service, the manager could monitor certain objects in the host device using SNMP traps to obtain usage information.

8.5 Configuration Management

Configuration management is the facilities to exercise control over a managed objects service. Within the MSE system, SNMP can be used, as well as, the IMS software ability to do some sort of remote procedure call. The IMS remote procedure call for Forward Error Correction (FEC) on and off is a remote software controlled configuration of the modems to turn on or off a software Forward error correction technique. The FEC on uses half of the available bandwidth to over come errors within the transmissions. Also, there is an RPC for conducting loops from modem to modem, which can be used in configuration or performance management. Another, configuration management technique used by MSE is to transfer Radio Access Unit (RAU) frequency plans from the system control center to the Group Logic Unit (GLU) of the RAU and from the GLU to the subscribers radio terminals. This transfer is done using the SCC' s connection to the Time Division Switching Group (TDSG) and then to the GLU signaling channel.

8.6 Performance Management

Performance management is the facilities or process of evaluation behavior of managed objects and the effectiveness on communications. MSE again uses SNMP (v1) as well as ICMP to derive the managed objects (Packet switches and high priority Hosts) with status information such as packet loss, up down status, software configuration and utilization. Another way MSE does performance management is through the IMS remote procedure call for remote configuration of propagation delay.

8.7 Security Management

Security management is the facilities or process that address security of managed objects. Since the MSE network has no managed objects with security features. The network has no facilities to manage security features such as the keys being used or which keys have been updated.

9. Conclusion

Future Army communicators will use models to engineer, monitor, validate and restore Army, Joint, and commercial telecommunications systems and interconnect these systems when required. Even with the advent of WIN-T, we believe that MSE and / or some other legacy system will continue to provide services to subscribers in some way (coalition armies, Reserve Components, etc.) on the future battlefield. The MSE network is complex and is presented to Army communicators at the Signal School using a component model rather than a layered, functional model. By describing MSE using a layered, functional model, future Army communicators will have the tools to quickly assimilate and understand any telecommunications system and how different systems interconnect.

This record demonstrates that the functional areas within MSE can be fully described using a common, standard model. The results of our research further show that this "systems modeling approach" allows students of telecommunications systems to quickly and more fully comprehend several complex telecommunications systems in a short period of time.

As the Army continues its transformation to a digitized force, future Army communicators must quickly assimilate and understand both legacy and future systems. Based on our research, it is our belief that this "systems modeling approach" is the only way to present several complex communications systems to a student with little background or experience and produce a professional, educated officer of the Signal Regiment.

Appendix A (MSE Functional Model Diagrams and Figures)

Figure 1.1 Basic Telecommunication Model

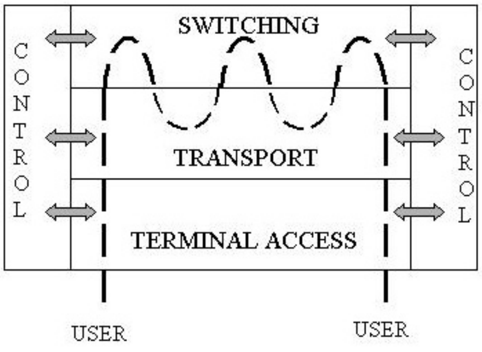


Figure 1.2 B-ISDN Layered Model

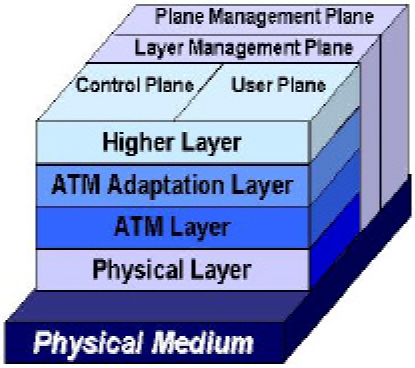
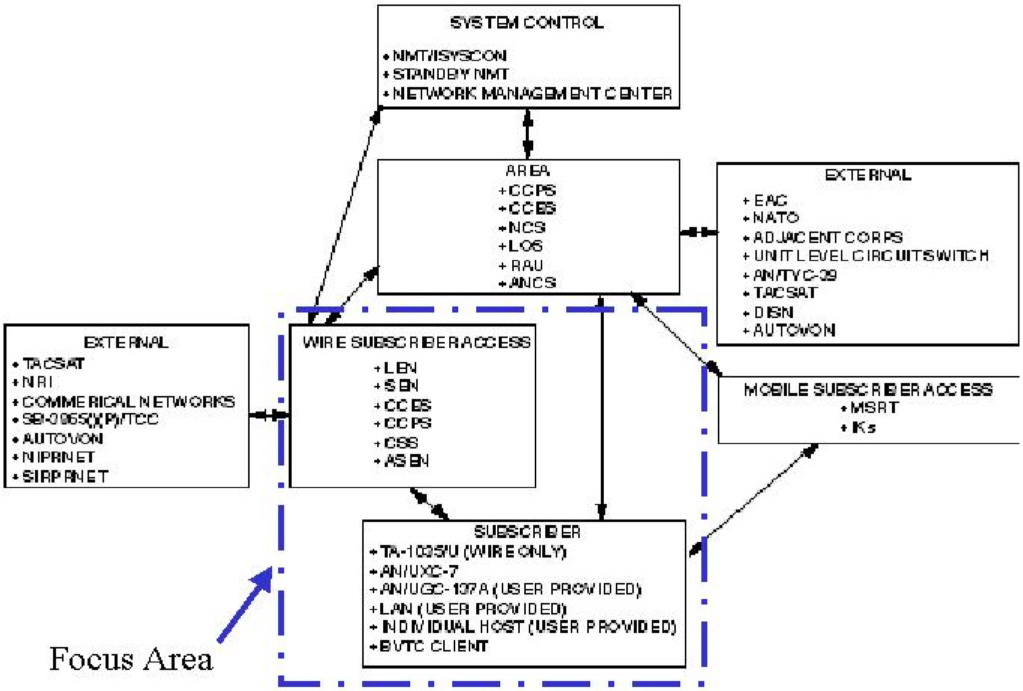
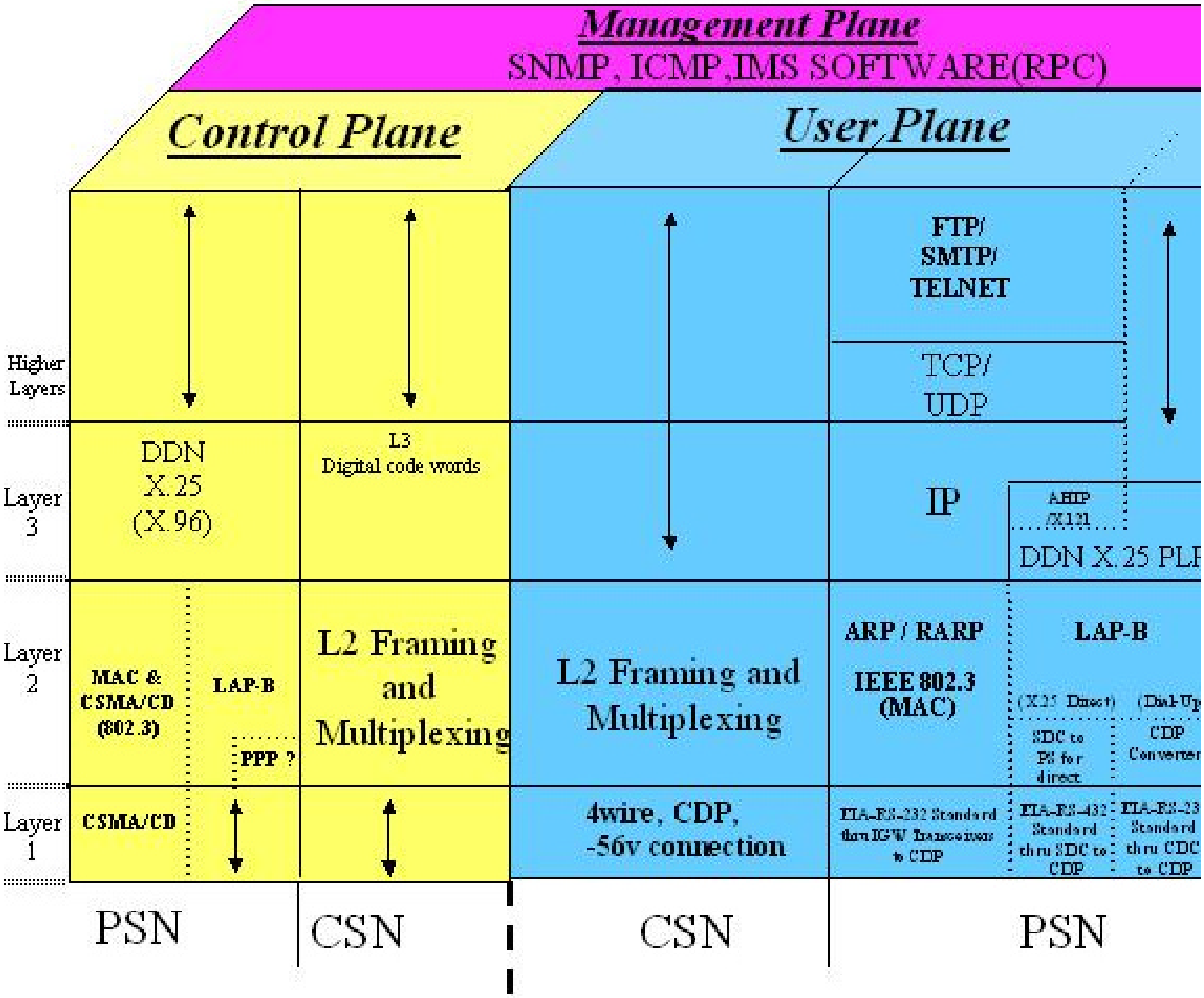


Figure 1.3 MSE Functional Areas



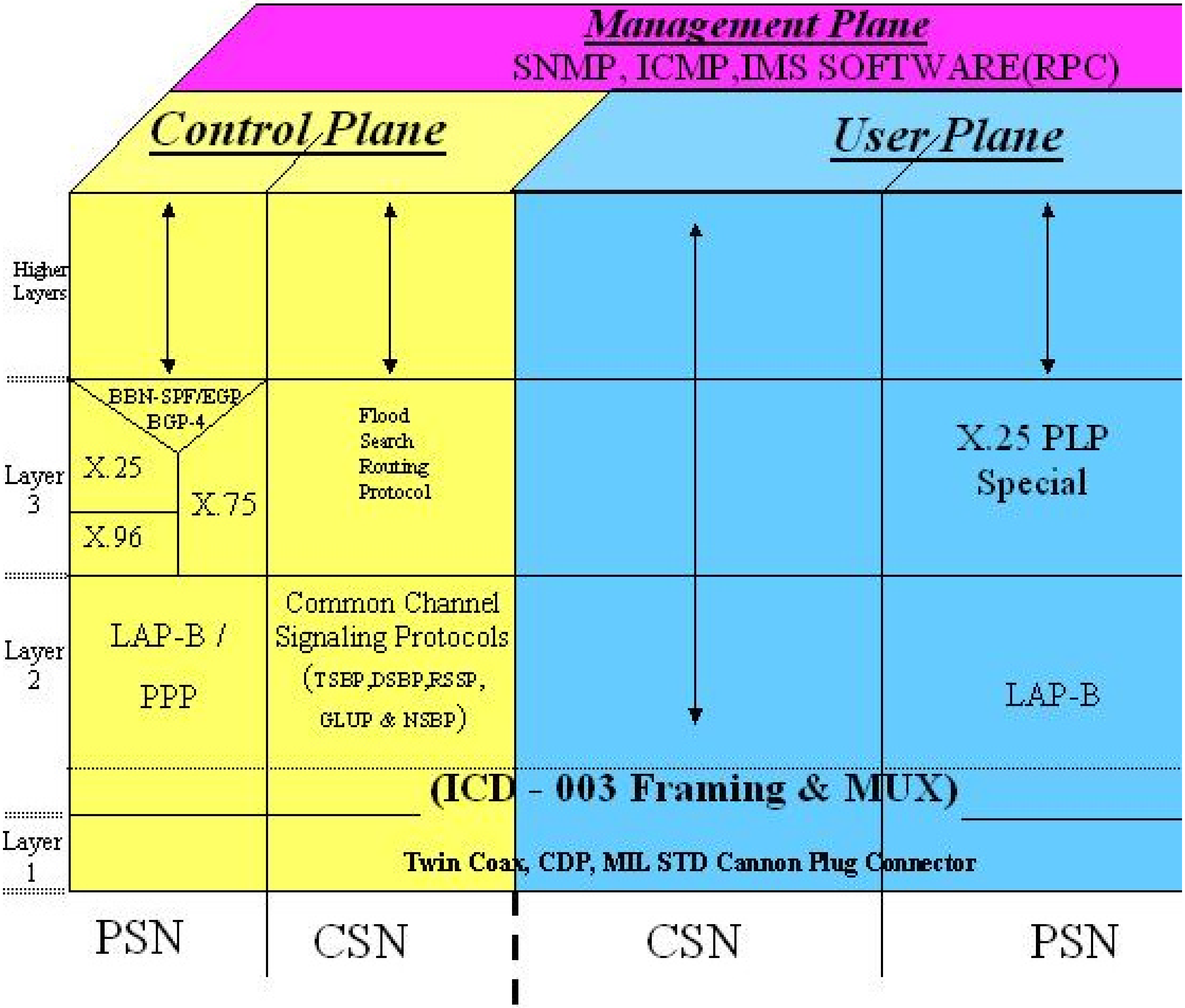
Appendix A (MSE Functional Model Diagrams and Figures)

Figure 1.4a Thesis MSE Protocol Reference Model (User to Network Interface)



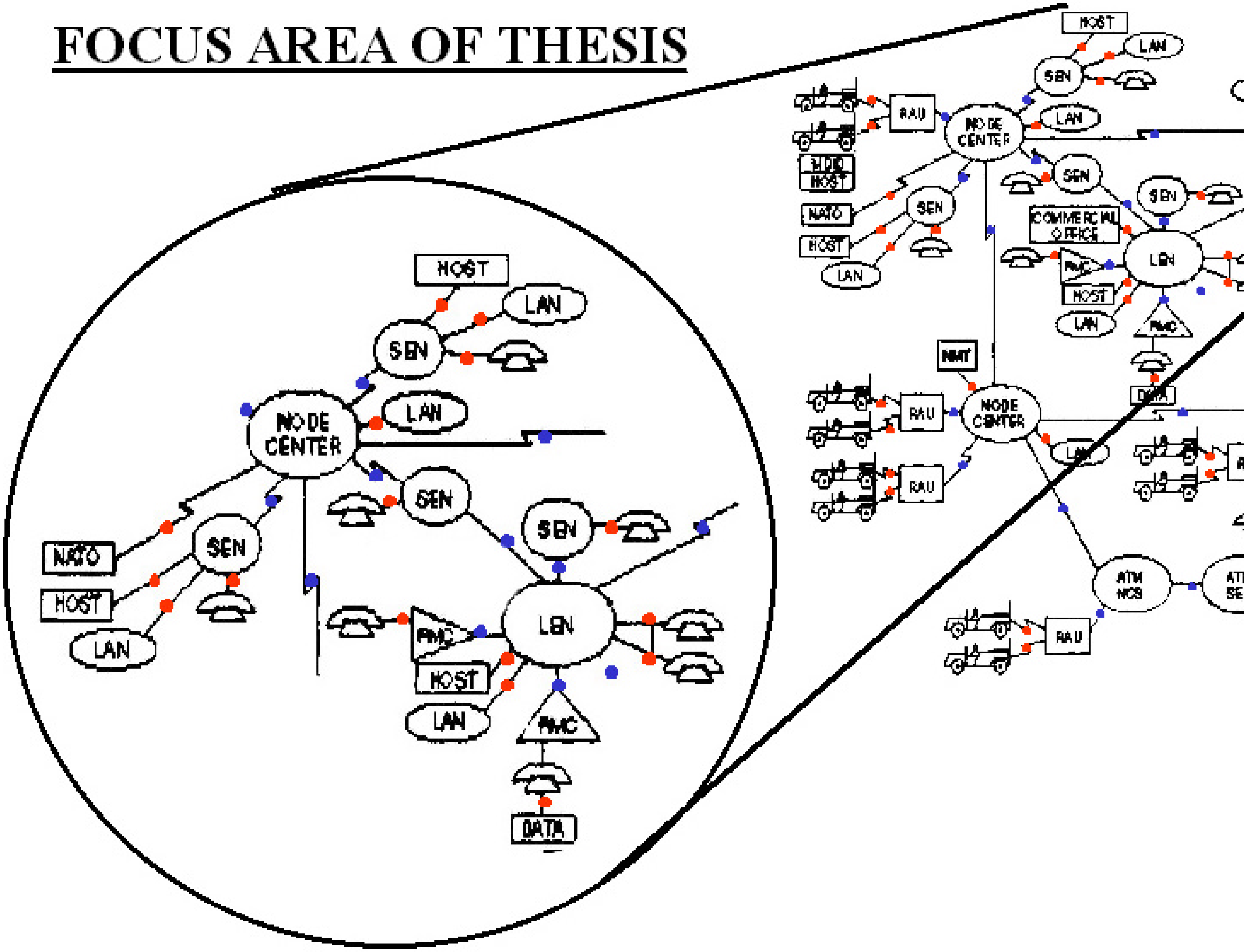
Appendix A (MSE Functional Model Diagrams and Figures)

Figure 1.4b Thesis MSE Protocol R eference Model (Network to Network Interface)


Management Plane
SNMP, ICMP,IMS SOFTWARE(RPC)
Control Plane
User Plane
Higher Layers
Layer 3
Layer 2
Layer 1
BBN-SPF/EGP
BGP-4
X.25
X.96
X.75
Flood Search Routing Protocol
X.25 PLP Special
LAP-B / PPP
Common Channel Signaling Protocols (TSBP,DSBP,RSSP, GLUP & NSBP)
LAP-B
(ICD - 003 Framing & MUX)
Twin Coax, CDP, MIL STD Cannon Plug Connector
PSN
CSN
CSN
PSN

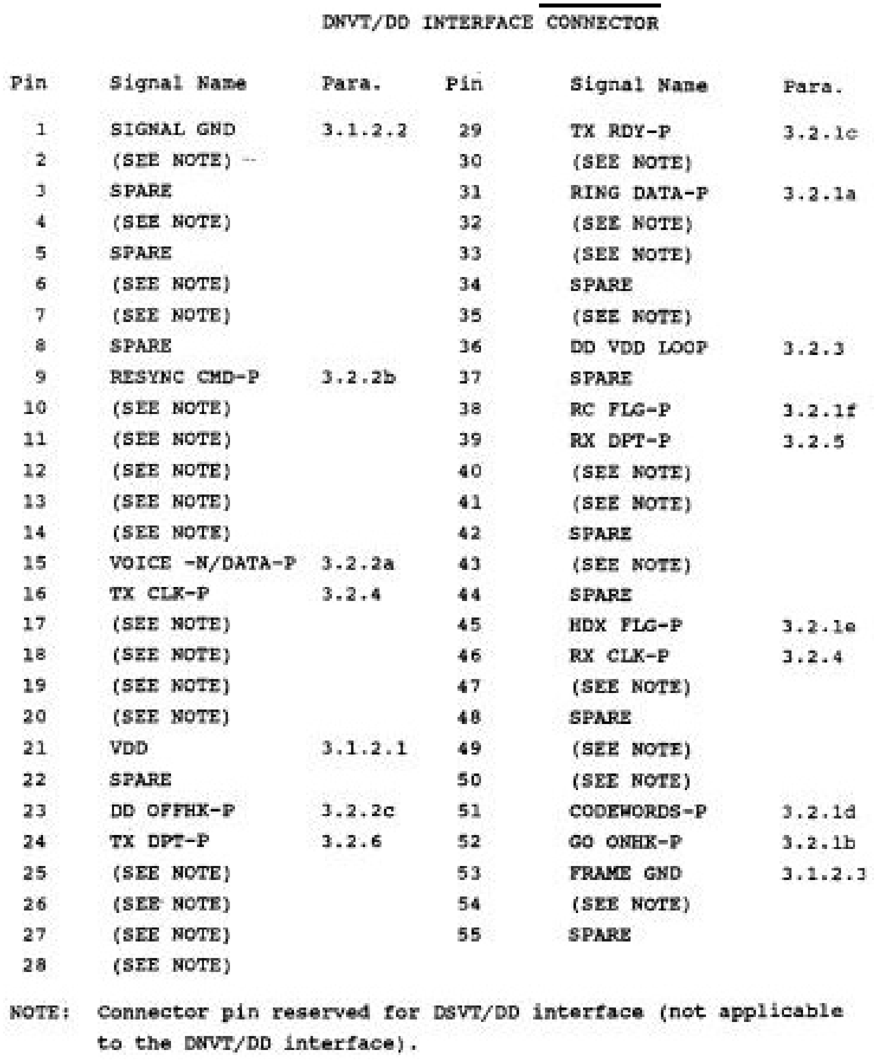
Appendix A (MSE Functional Model Diagrams and Figures)

Figure 1.5 Thesis UNI and NNI Focus Area



Appendix B (CSN Tables, Diagrams and Figures)

__Table B1__



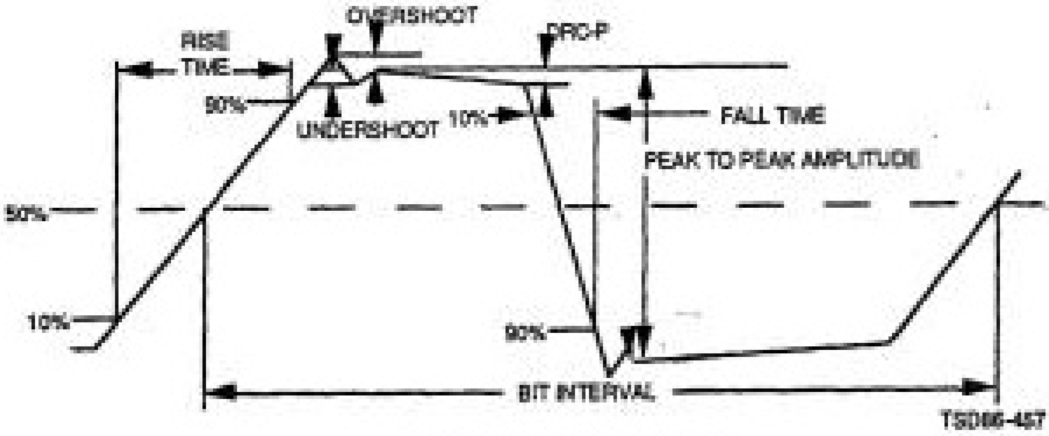
DNVT/DD INTERFACE CONNECTOR

Pin	Signal Name	Para.	Pin	Signal Name	Para.
1	SIGNAL GND	3.1.2.2	29	TX RDY-P	3.2.1c
2	(SEE NOTE) --		30	(SEE NOTE)	
3	SPARE		31	RING DATA-P	3.2.1a
4	(SEE NOTE)		32	(SEE NOTE)	
5	SPARE		33	(SEE NOTE)	
6	(SEE NOTE)		34	SPARE	
7	(SEE NOTE)		35	(SEE NOTE)	
8	SPARE		36	DD VDD LOOP	3.2.3
9	RESYNC CMD-P	3.2.2b	37	SPARE	
10	(SEE NOTE)		38	RC FLG-P	3.2.1f
11	(SEE NOTE)		39	RX DPT-P	3.2.5
12	(SEE NOTE)		40	(SEE NOTE)	
13	(SEE NOTE)		41	(SEE NOTE)	
14	(SEE NOTE)		42	SPARE	
15	VOICE -N/DATA-P	3.2.2a	43	(SEE NOTE)	
16	TX CLK-P	3.2.4	44	SPARE	
17	(SEE NOTE)		45	HDX FLG-P	3.2.1e
18	(SEE NOTE)		46	RX CLK-P	3.2.4
19	(SEE NOTE)		47	(SEE NOTE)	
20	(SEE NOTE)		48	SPARE	
21	VDD	3.1.2.1	49	(SEE NOTE)	
22	SPARE		50	(SEE NOTE)	
23	DD OFFHK-P	3.2.2c	51	CODEWORDS-P	3.2.1d
24	TX DPT-P	3.2.6	52	GO ONHK-P	3.2.1b
25	(SEE NOTE)		53	FRAME GND	3.1.2.3
26	(SEE NOTE)		54	(SEE NOTE)	
27	(SEE NOTE)		55	SPARE	
28	(SEE NOTE)				

NOTE: Connector pin reserved for DSVT/DD interface (not applicable to the DNVT/DD interface).

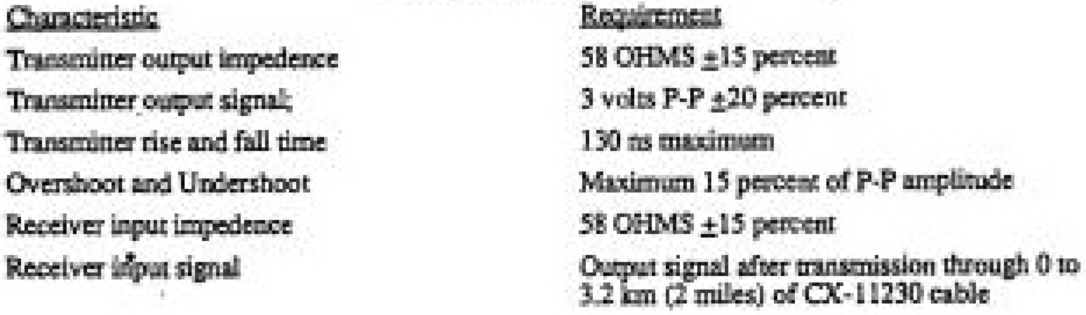
Appendix B (CSN Tables, Diagrams and Figures)

Figure B1



Typical Diphase Waveform

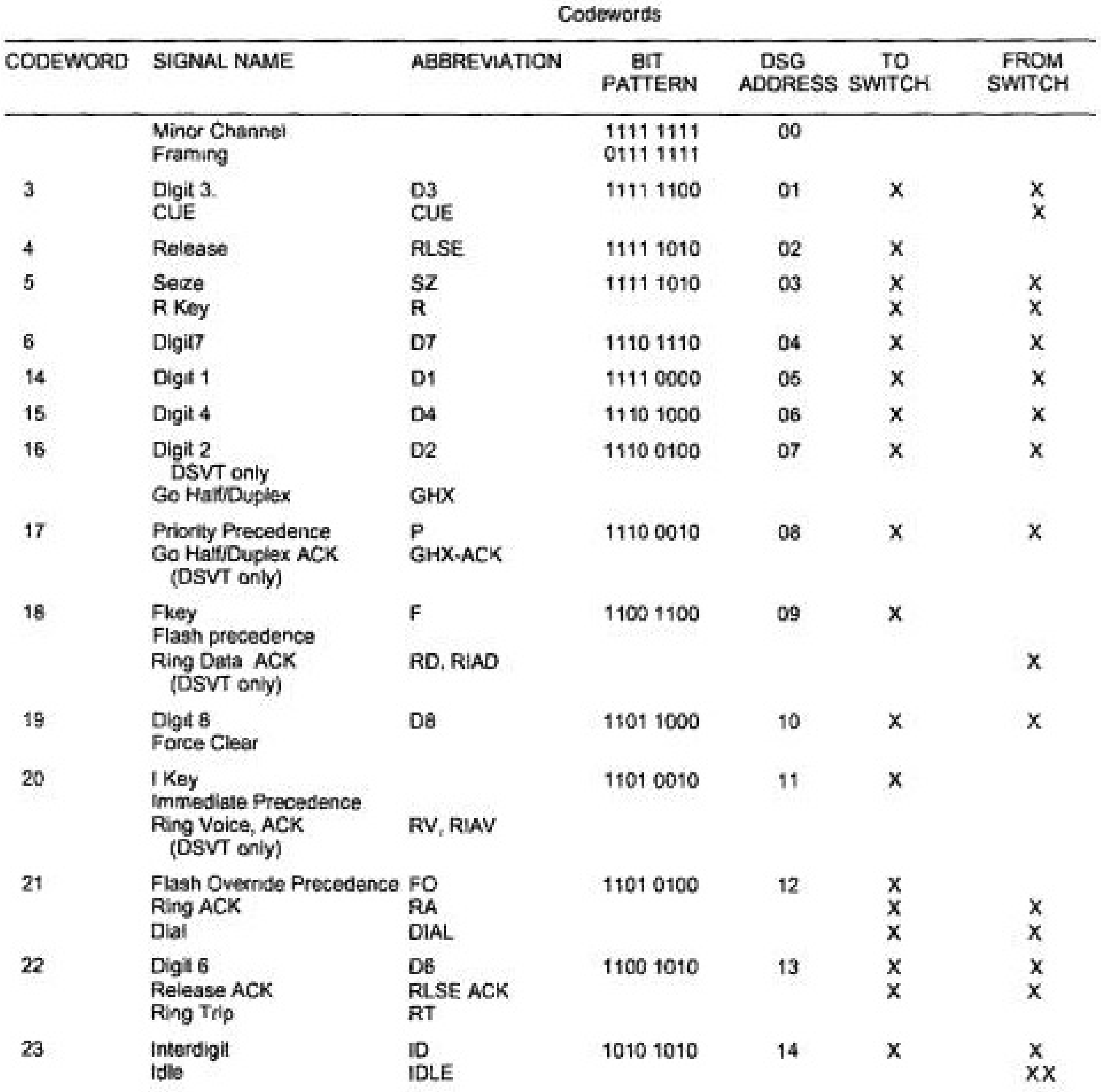
Transmission Characteristics



Characteristic	Requirement
Transmitter output impedence	58 OHMS ±15 percent
Transmitter output signal;	3 volts P-P ±20 percent
Transmitter rise and fall time	130 ns maximum
Overshoot and Undershoot	Maximum 15 percent of P-P amplitude
Receiver input impedence	58 OHMS ±15 percent
Receiver input signal	Output signal after transmission through 0 to 3.2 km (2 miles) of CX-11230 cable

Appendix B (CSN Tables， Diagrams and Figures)

Table B2

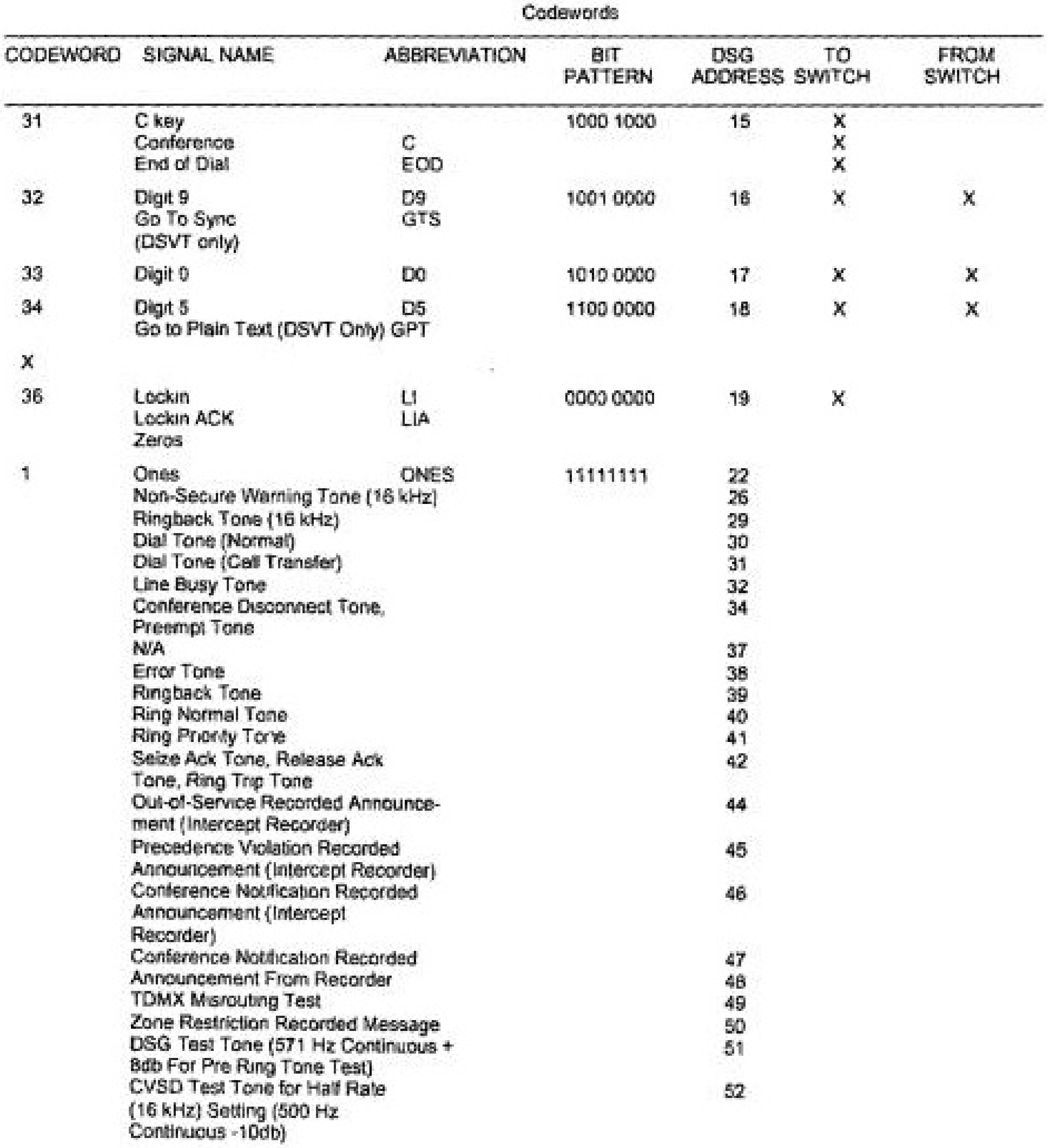


Codewords

CODEWORD	SIGNAL NAME	ABBREVIATION	BIT PATTERN	DSG ADDRESS	TO SWITCH	FROM SWITCH
	Minor Channel		1111 1111	00		
	Framing		0111 1111			
3	Digit 3.	D3	1111 1100	01	X	X
	CUE	CUE				X
4	Release	RLSE	1111 1010	02	X	
5	Seze	SZ	1111 1010	03	X	X
	R Key	R			X	X
6	Digit7	D7	1110 1110	04	X	X
14	Digit 1	D1	1111 0000	05	X	X
15	Digit 4	D4	1110 1000	06	X	X
16	Digit 2	D2	1110 0100	07	X	X
	DSVT only					
	Go Half/Duplex	GHX				
17	Priority Precedence	P	1110 0010	08	X	X
	Go Half/Duplex ACK	GHX-ACK				
	(DSVT only)					
18	Fkey	F	1100 1100	09	X	
	Flash precedence					
	Ring Data ACK	RD, RIAD				X
	(DSVT only)					
19	Digit 8	D8	1101 1000	10	X	X
	Force Clear					
20	I Key		1101 0010	11	X	
	Immediate Precedence					
	Ring Voice, ACK	RV, RIAV				
	(DSVT only)					
21	Flash Overnde Precedence	FO	1101 0100	12	X	
	Ring ACK	RA			X	X
	Dial	DIAL			X	X
22	Digit 6	D6	1100 1010	13	X	X
	Release ACK	RLSE ACK			X	X
	Ring Trip	RT				
23	Interdigit	ID	1010 1010	14	X	X
	Idle	IDLE				XX

Appendix B (CSN Tables, Diagrams and Figures)

Table B3

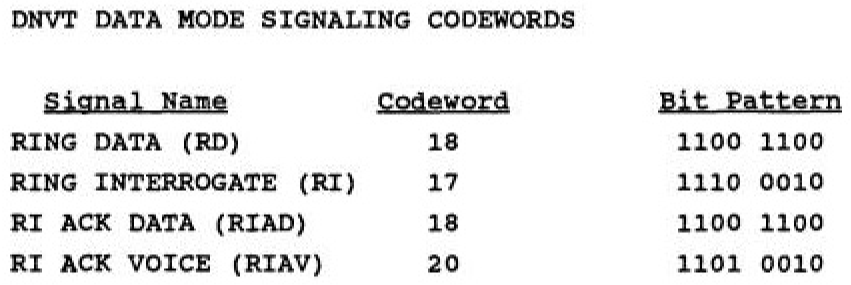


Codewords

CODEWORD	SIGNAL NAME	ABBREVIATION	BIT PATTERN	DSG ADDRESS	TO SWITCH	FROM SWITCH
31	C key		1000 1000	15	X	
	Conference	C			X	
	End of Dial	EOD			X	
32	Digit 9	D9	1001 0000	16	X	X
	Go To Sync (DSVT only)	GTS				
33	Digit 0	D0	1010 0000	17	X	X
34	Digt 5	D5	1100 0000	18	X	X
	Go to Plain Text (DSVT Only)	GPT				
X						
36	Lockin	LI	0000 0000	19	X	
	Lockin ACK	LIA				
	Zeros					
1	Ones	ONES	11111111	22		
	Non-Secure Warning Tone (16 kHz)			26		
	Ringback Tone (16 kHz)			29		
	Dial Tone (Normal)			30		
	Dial Tone (Call Transfer)			31		
	Line Busy Tone			32		
	Conference Disconnect Tone, Preempt Tone			34		
	N/A			37		
	Error Tone			38		
	Ringback Tone			39		
	Ring Normal Tone			40		
	Ring Priority Tone			41		
	Seize Ack Tone, Release Ack Tone, Ring Trip Tone			42		
	Out-of-Service Recorded Announcement (Intercept Recorder)			44		
	Precedence Violation Recorded Announcement (Intercept Recorder)			45		
	Conference Notification Recorded Announcement (Intercept Recorder)			46		
	Conference Notification Recorded			47		
	Announcement From Recorder			48		
	TDMX Misrouting Test			49		
	Zone Restriction Recorded Message			50		
	DSG Test Tone (571 Hz Continuous + 8db For Pre Ring Tone Test)			51		
	CVSD Test Tone for Half Rate (16 kHz) Setting (500 Hz Continuous -10db)			52		

Appendix B (CSN Tables, Diagrams and Figures)

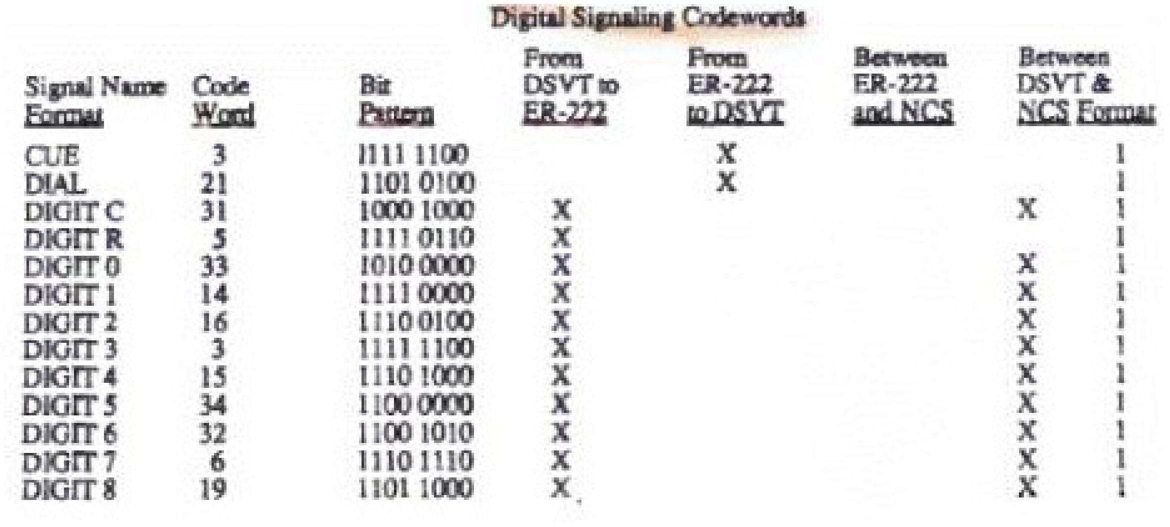
Table B4



DNVT DATA MODE SIGNALING CODEWORDS

Signal Name	Codeword	Bit Pattern
RING DATA (RD)	18	1100 1100
RING INTERROGATE (RI)	17	1110 0010
RI ACK DATA (RIAD)	18	1100 1100
RI ACK VOICE (RIAV)	20	1101 0010

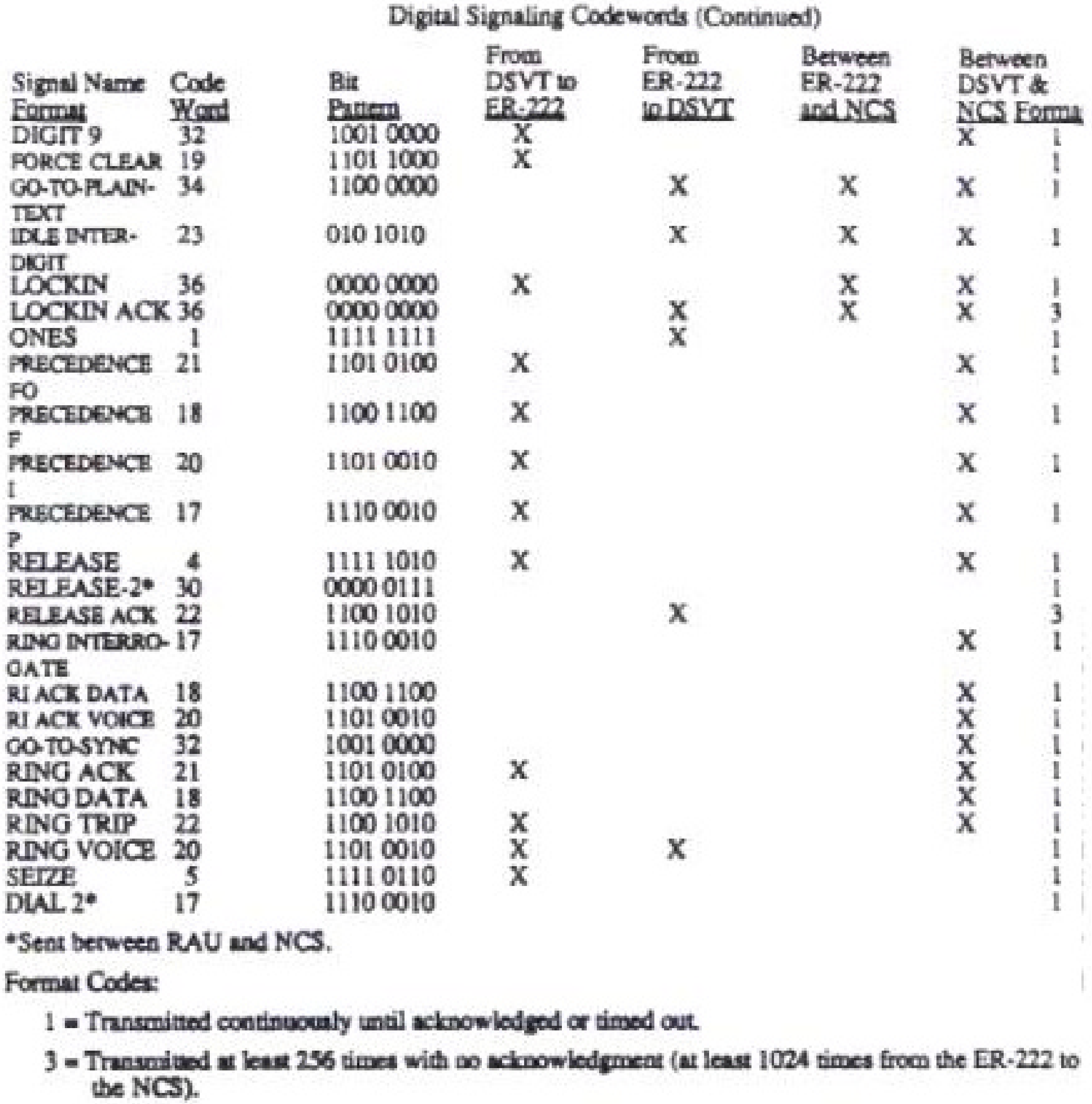
Table B5



Digital Signaling Codewords

Signal Name Format	Code Word	Bit Pattern	From DSVT to ER-222	From ER-222 to DSVT	Between ER-222 and NCS	Between DSVT & NCS	Format
CUE	3	1111 1100		X			1
DIAL	21	1101 0100		X			1
DIGIT C	31	1000 1000	X			X	1
DIGIT R	5	1111 0110	X				1
DIGIT 0	33	1010 0000	X			X	1
DIGIT 1	14	1111 0000	X			X	1
DIGIT 2	16	1110 0100	X			X	1
DIGIT 3	3	1111 1100	X			X	1
DIGIT 4	15	1110 1000	X			X	1
DIGIT 5	34	1100 0000	X			X	1
DIGIT 6	32	1100 1010	X			X	1
DIGIT 7	6	1110 1110	X			X	1
DIGIT 8	19	1101 1000	X			X	1

Table B6



Digital Signaling Codewords (Continued)

Signal Name Format	Code Word	Bit Pattern	From DSVT to ER-222	From ER-222 to DSVT	Between ER-222 and NCS	Between DSVT & NCS	Forma
DIGIT 9	32	1001 0000	X			X	1
FORCE CLEAR	19	1101 1000	X				1
GO-TO-PLAIN-TEXT	34	1100 0000		X	X	X	1
IDLE INTER-DIGIT	23	010 1010		X	X	X	1
LOCKIN	36	0000 0000	X		X	X	1
LOCKIN ACK	36	0000 0000		X	X	X	3
ONES	1	1111 1111		X			1
PRECEDENCE FO	21	1101 0100	X			X	1
PRECEDENCE F	18	1100 1100	X			X	1
PRECEDENCE I	20	1101 0010	X			X	1
PRECEDENCE P	17	1110 0010	X			X	1
RELEASE	4	1111 1010	X			X	1
RELEASE-2*	30	0000 0111					1
RELEASE ACK	22	1100 1010		X			3
RING INTERRO-GATE	17	1110 0010				X	1
RI ACK DATA	18	1100 1100				X	1
RI ACK VOICE	20	1101 0010				X	1
GO-TO-SYNC	32	1001 0000				X	1
RING ACK	21	1101 0100	X			X	1
RING DATA	18	1100 1100				X	1
RING TRIP	22	1100 1010	X			X	1
RING VOICE	20	1101 0010	X	X			1
SEIZE	5	1111 0110	X				1
DIAL 2*	17	1110 0010					1

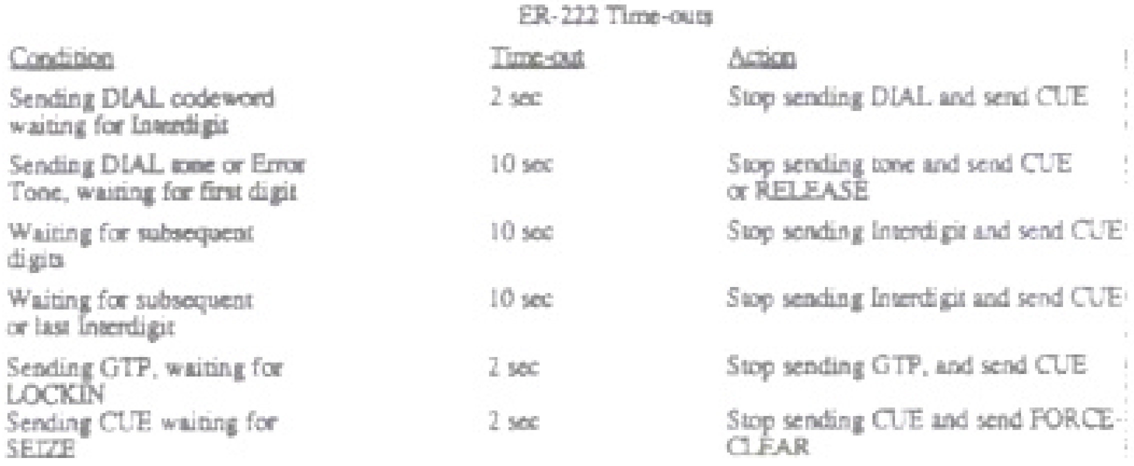
*Sent between RAU and NCS.

Format Codes:

1 = Transmitted continuously until acknowledged or timed out.

3 = Transmitted at least 256 times with no acknowledgment (at least 1024 times from the ER-222 to the NCS).

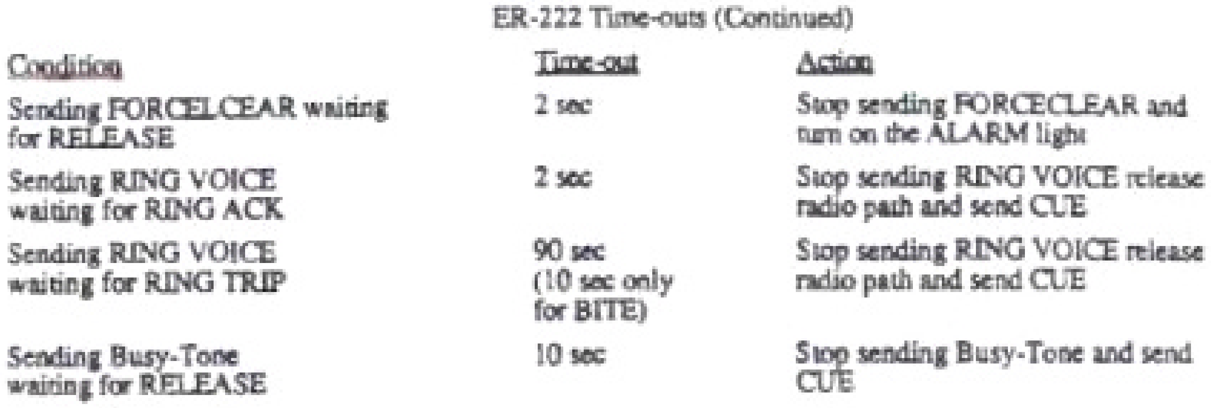
Table B7



ER-222 Time-outs

Condition	Time-out	Action
Sending DIAL codeword waiting for Interdigit	2 sec	Stop sending DIAL and send CUE
Sending DIAL tone or Error Tone, waiting for first digit	10 sec	Stop sending tone and send CUE or RELEASE
Waiting for subsequent digits	10 sec	Stop sending Interdigit and send CUE
Waiting for subsequent or last Interdigit	10 sec	Stop sending Interdigit and send CUE
Sending GTP, waiting for LOCKIN	2 sec	Stop sending GTP, and send CUE
Sending CUE waiting for SEIZE	2 sec	Stop sending CUE and send FORCE-CLEAR

Table B8



ER-222 Time-outs (Continued)

Condition	Time-out	Action
Sending FORCELCEAR waiting for RELEASE	2 sec	Stop sending FORCECLEAR and turn on the ALARM light
Sending RING VOICE waiting for RING ACK	2 sec	Stop sending RING VOICE release radio path and send CUE
Sending RING VOICE waiting for RING TRIP	90 sec (10 sec only for BITE)	Stop sending RING VOICE release radio path and send CUE
Sending Busy-Tone waiting for RELEASE	10 sec	Stop sending Busy-Tone and send CUE

Appendix B (CSN Tables，Diagrams and Figures)

Figure B2

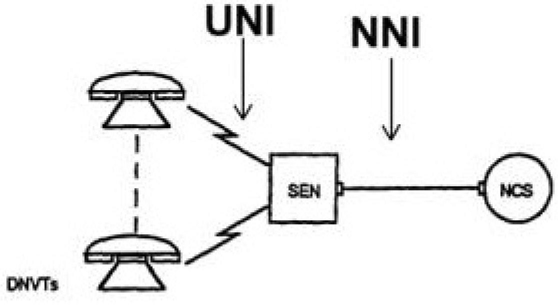
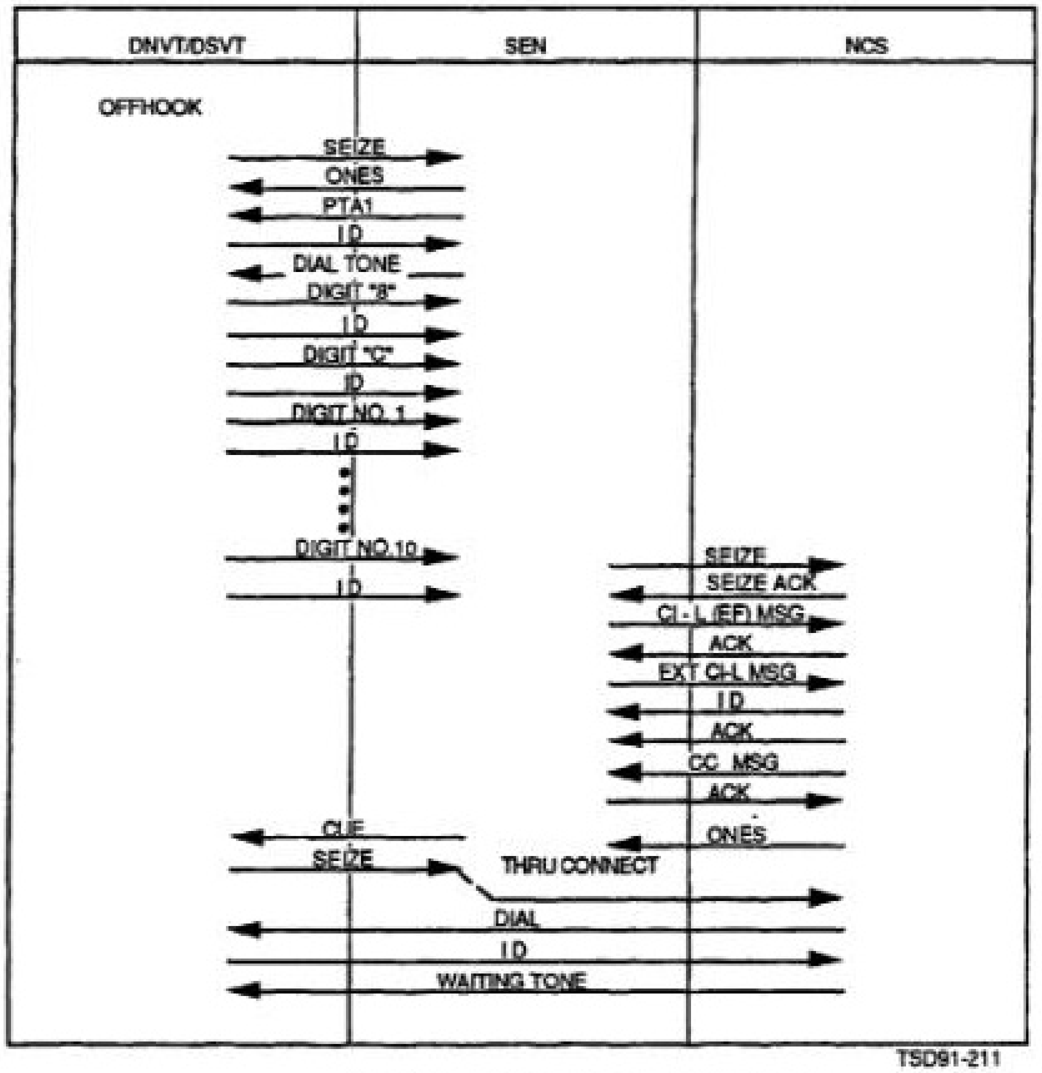


Figure B3



TSD91-211

Subscriber Disaffiliation (Initiation Phase)

THIS PAGE LEFT INTENTIONALLY BLANK

THIS PAGE LEFT INTENTIONALLY BLANK

Fig 1. Network -to-Network Interfaces

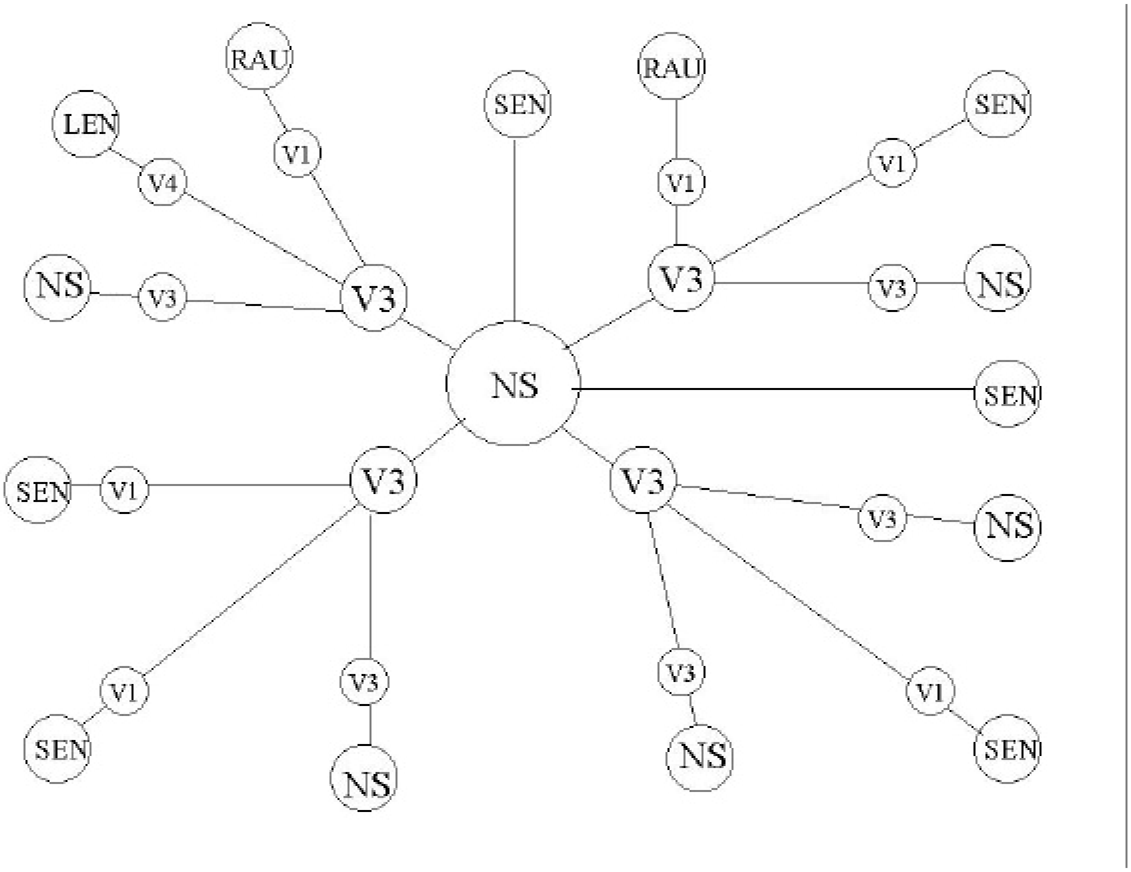
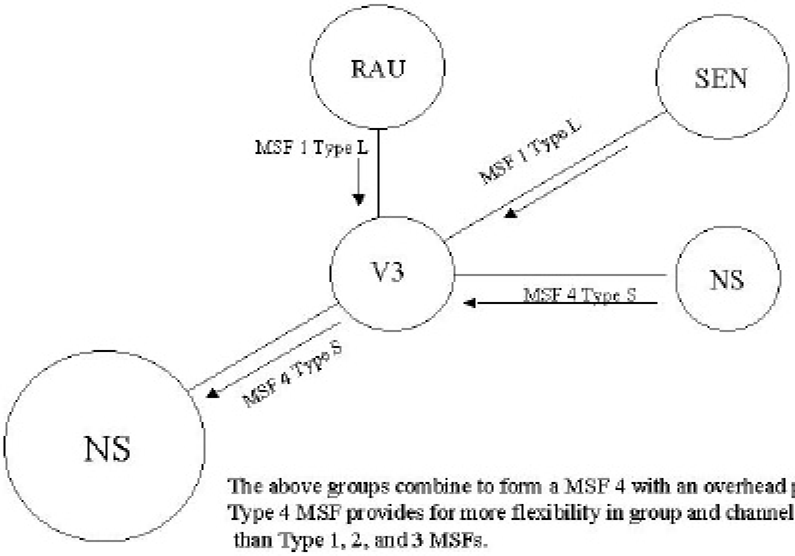
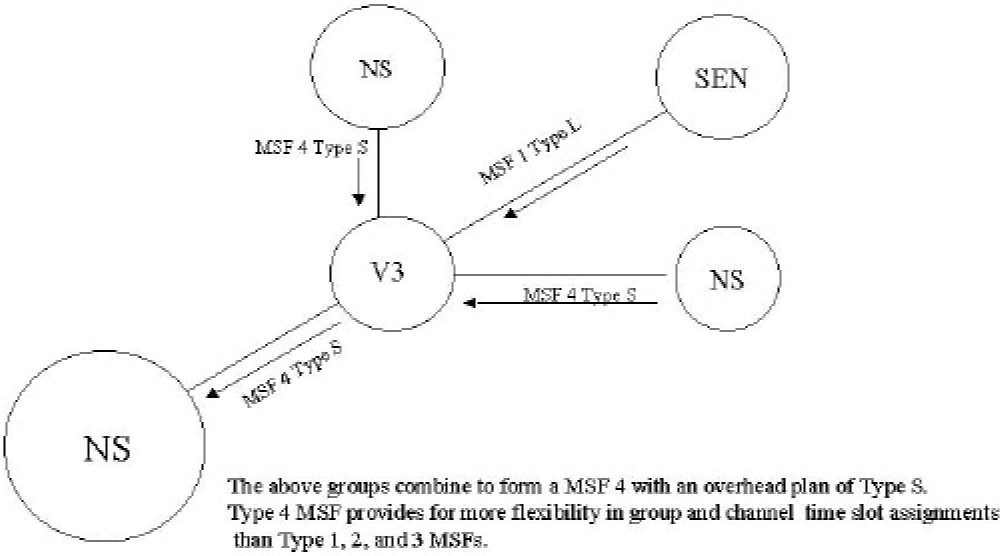


Fig 2. Network -to-Network Interfaces



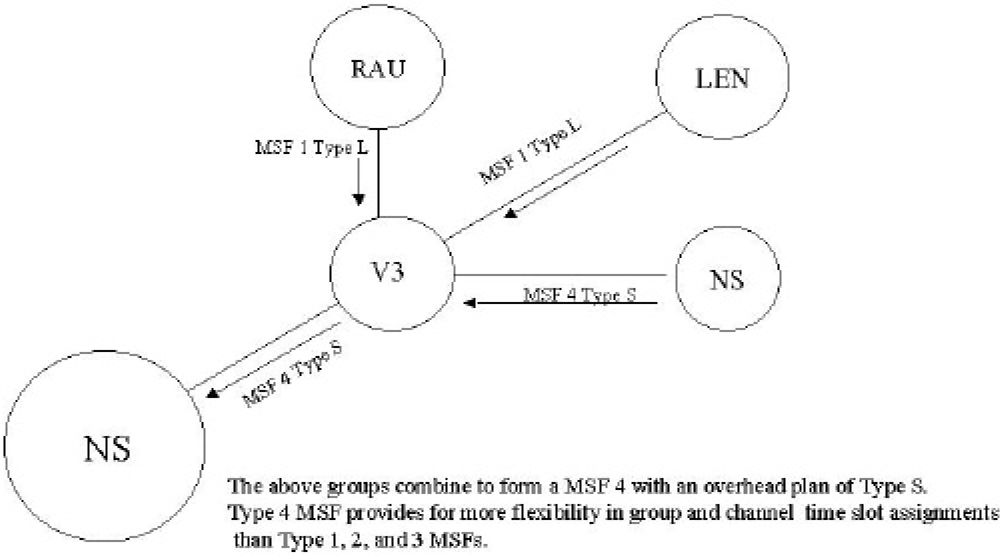
The above groups combine to form a MSF 4 with an overhead plan of Type S.
Type 4 MSF provides for more flexibility in group and channel time slot assignments than Type 1, 2, and 3 MSFs.

Fig 3. Network -to-Network Interfaces



The above groups combine to form a MSF 4 with an overhead plan of Type S.
Type 4 MSF provides for more flexibility in group and channel time slot assignments than Type 1, 2, and 3 MSFs.

Fig 4. Network -to-Network Interfaces



The above groups combine to form a MSF 4 with an overhead plan of Type S.
Type 4 MSF provides for more flexibility in group and channel time slot assignments than Type 1, 2, and 3 MSFs.

Fig 5. Multiplex Signal Format 1

Type 1 MSF. The type 1 MSF is organized to use a single L, O, or S type overhead plan providing a time slot structure for one primary overhead channel and from 7 to 143 traffic channels.

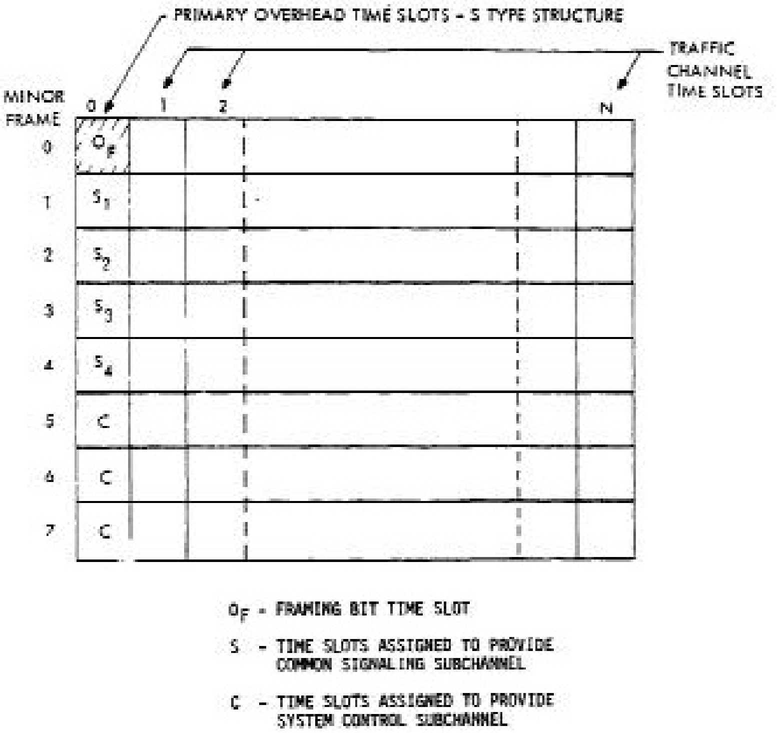
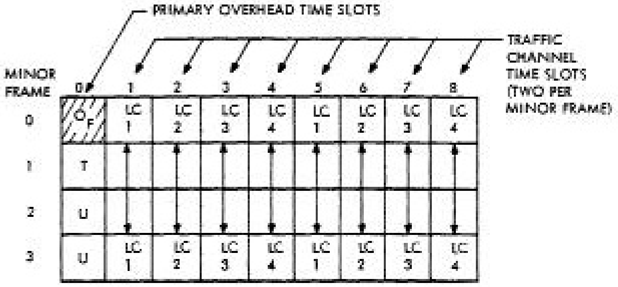

PRIMARY OVERHEAD TIME SLOTS – S TYPE STRUCTURE
TRAFFIC CHANNEL TIME SLOTS
MINOR FRAME
0
1
2
N
0
1
2
3
4
5
6
7
O_F
S_1
S_2
S_3
S_4
C
C
C
O_F – FRAMING BIT TIME SLOT
S – TIME SLOTS ASSIGNED TO PROVIDE COMMON SIGNALING SUBCHANNEL
C – TIME SLOTS ASSIGNED TO PROVIDE SYSTEM CONTROL SUBCHANNEL

Figure 8. Type 1 MSF with Signaling Subchannel

Fig 6. Multiplex Sign al Format 2

The Type 2 MSF utilizes four minor frames and provides a time slot structure to accommodate an L-type overhead plan and four traffic channels. A minor frame consists of one time slot for the overhead channel followed by two time slots for each of the four traffic channels.



ORDER OF TRANSMISSION IS LEFT TO RIGHT
TOP TO BOTTOM

O_F - FRAMING BIT TIME SLOT

T - TIME SLOT ASSIGNED FOR
TELEMETRY SUBCHANNEL 2/4 kb/s

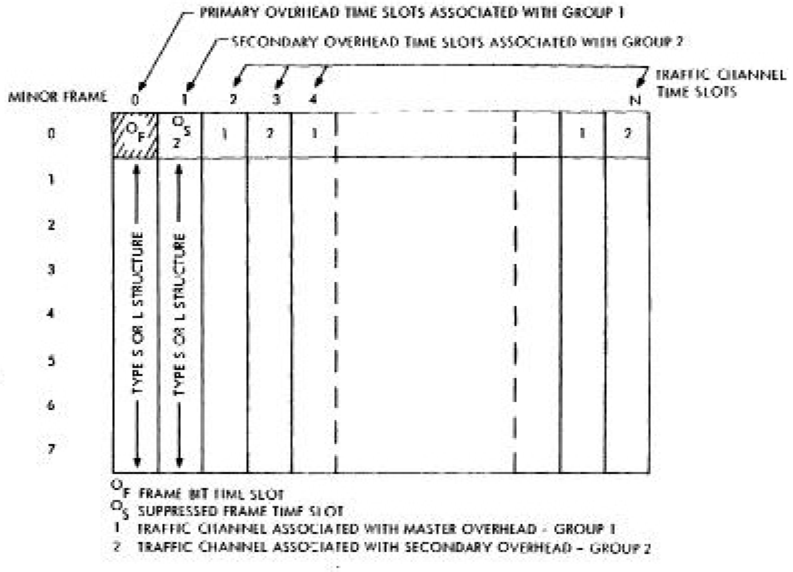
U - NOT USED

LC - LOCAL CHANNEL

Figure 20. Type 2 Multiplex Signal Format

Fig 7. Multiplex Signal Format 3

Type 3 MSFs are used on the supergroup side of a TGM and can also be used on groups originating in the AN/TTC-39 series CS. Type 3 MSF provides capacity for combining groups of channels up to maximum DTG capacity using a single MSF having a total time slot capacity of 16,32, 48, 64 and 128 or 18, 36, 72, and 144. The first group is a multiple of 8 and the second group a multiple of 9. The framing bit time slot must contain an 1100 sequence and not a 1010 sequence. When the Secondary Overhead plans are an S-type plan, the common signaling sub-channel serves the traffic channels with which they are associated. There are 5 Type 3 Formats: 3A1, 3A2, 3A3, 3B and 3C. The overhead time slot structure of a Type 3 MSF must be either an S or L plan. Each format is a bit rate plan for interleaving channel groups.


PRIMARY OVERHEAD TIME SLOTS ASSOCIATED WITH GROUP 1
SECONDARY OVERHEAD TIME SLOTS ASSOCIATED WITH GROUP 2
TRAFFIC CHANNEL TIME SLOTS
MINOR FRAME
0
1
2
3
4
N
0
1
2
3
4
5
6
7
O_F
O_S
2
1
2
1
1
2
TYPE S OR L STRUCTURE
TYPE S OR L STRUCTURE
O_F FRAME BIT TIME SLOT
O_S SUPPRESSED FRAME TIME SLOT
1 TRAFFIC CHANNEL ASSOCIATED WITH MASTER OVERHEAD - GROUP 1
2 TRAFFIC CHANNEL ASSOCIATED WITH SECONDARY OVERHEAD - GROUP 2

33

Figure 21. Type 3A1 Multiplex Signal Format

Fig 8. Multiplex Signal Format 4

Type 4 MSF provides capacity for combining groups of channels up to maximum DTG capacity using a single MSF having a total time slot capacity of 16,32, 48, 64 and 128 or 18, 36, 72, and 144. The first group is a multiple of 8 and the second group a multiple of 9. The framing bit time slot must contain an 1100 sequence and not a 1010 sequence. Any S or L type overhead channel plan associated with the groups to be combined may be selected to serve as the primary overhead structure for the major frame. Secondary overhead pans used to service the associated traffic channels must be positioned within the first time slots of the Type 4 MSF. There are three Type 4 Multiplex Signal Formats: Type 4A, Type 4B and Type 4C.

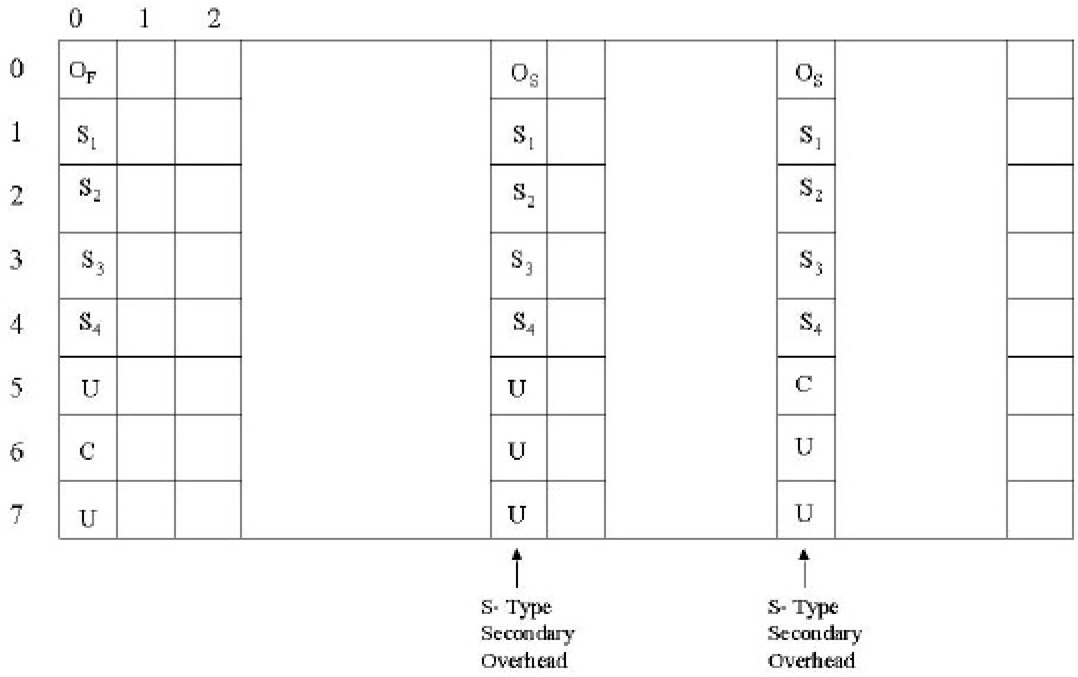
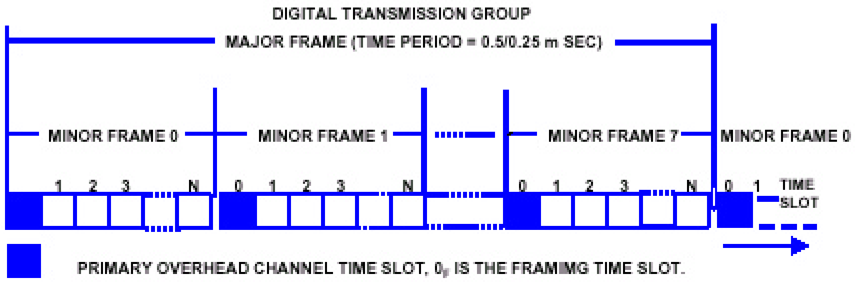


Fig 9. Bit Stream Representation of a Major Frame



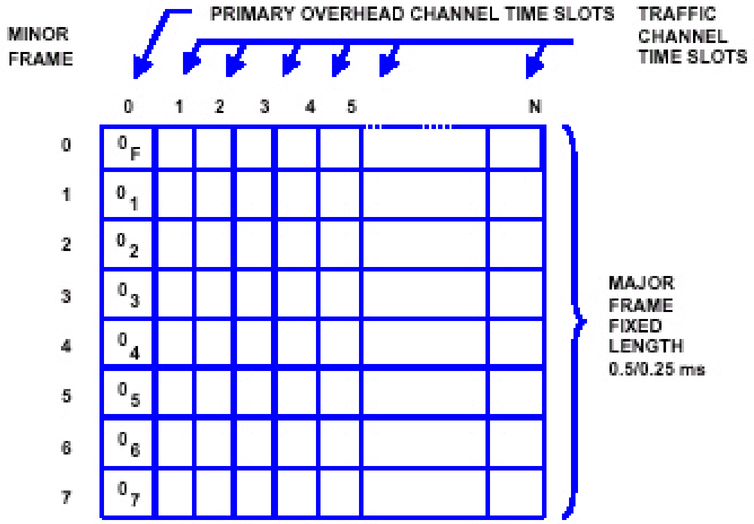
■ PRIMARY OVERHEAD CHANNEL TIME SLOT, 0_F IS THE FRAMIMG TIME SLOT.

□ TRAFFIC CHANNEL TIME SLOT.

MAJOR FRAME COMPOSED OF EIGHT MINOR FRAMES.

MIINOR FRAME ALLOCATES ONE TIME SLOT TO OVERHEAD CHANNEL AND ONE TIME SLOT TO EACH TRAFFIC CHANNEL, BIT INTERLACED.

RECTANGULAR ARRAY REPRESENTATION OF MAJOR FRAME ORGANIZATION

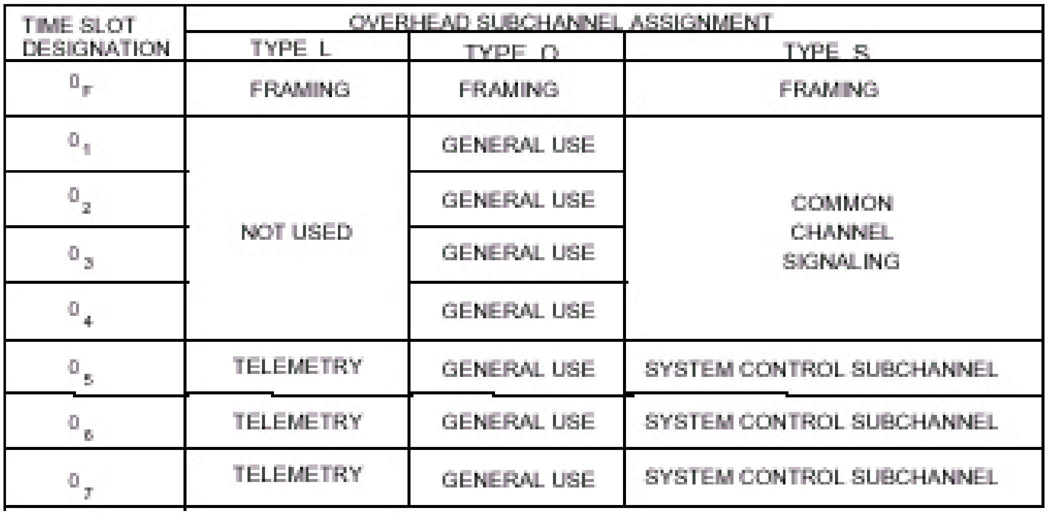

MINOR FRAME
PRIMARY OVERHEAD CHANNEL TIME SLOTS
TRAFFIC CHANNEL TIME SLOTS
0 1 2 3 4 5 N
0 1 2 3 4 5 6 7
0F
01
02
03
04
05
06
07
MAJOR FRAME FIXED LENGTH 0.5/0.25 ms

ORDER OF TRANSMISSION IS LEFT TO RIGHT, TOP TO BOTTOM.

RECTANGULAR ARRAY PRESENTATION OF MAJOR FRAME ORGANIZATION.

Overhead Time Slot Assignments For Each Type Plan

There are three primary overhead channelization plans designated as Type L, Type O, and Type S which define particular time slot to sub-channel assignment. Both Type S and Type L plans reserve time slots 05, 06, and 07 for system control or telemetry use. In an S type plan, these time slots are generally used for message interchange. In an L type plan, these time slots are used for loopback tests between DGM equipment. The primary overhead time slot structure consists of the framing bit time slot with either three or seven time slots that may be used to provide up to three or seven subchannels operating at the 2- or 4-Kbps rate.



TIME SLOT DESIGNATION	OVERHEAD SUBCHANNEL ASSIGNMENT		
	TYPE L	TYPE O	TYPE S
0_F	FRAMING	FRAMING	FRAMING
0_1	NOT USED	GENERAL USE	COMMON CHANNEL SIGNALING
0_2		GENERAL USE	
0_3		GENERAL USE	
0_4		GENERAL USE	
0_5	TELEMETRY	GENERAL USE	SYSTEM CONTROL SUBCHANNEL
0_6	TELEMETRY	GENERAL USE	SYSTEM CONTROL SUBCHANNEL
0_7	TELEMETRY	GENERAL USE	SYSTEM CONTROL SUBCHANNEL

The L-Type Plan - The first four time slots are unused and the fifth, sixth, and seventh time slots are assigned to provide three separate telemetry sub-channels.

The O-Type Plan - The seven time slots are for general use.

The S-Type Plan - The first four time slots form the common signaling sub-channel and the fifth, sixth, and seventh time slots are assigned to provide three separate system control sub-channels.

The system control and telemetry sub-channels provide an information rate of 2 kb/s. The sub-channel rates are 2 kb/s for a voice digitization rate of 16 kb/s and 4 kb/s for a voice digitization rate of 32 kb/s. The common signaling sub-channel operates at an 8 kb/s rate for a voice digitization rate of 16 kb/s and 16 kb/s rate for a voice digitization rate of 32 kb/s.

C.2 Multiplex Signal Format Architectures

Multiplex Signal Formats are organized into four basic types and provide transmission capabilities required by a broad set of applications. These applications dictate specific arrangements of the Multiplex Signal Formats in terms of the time slot to channel assignments. All Multiplex Signal Formats use a fixed length frame, defined by a framing bit and a series of sequential information bits. The common frame plan assigns the first time slot in each frame as the framing bit. From one frame to the next, this framing bit produces the in-sync frame pattern consisting of an alternating one-zero (1010) sequence at a 2- or 4-Kbps rate. These frame bits define the beginning of each new frame of time slots that are associated with the individual channels. The bits contained in each time slot are demultiplexed by mutual synchronization between time slot assignments. The fixed length frame is defined as a major frame. All DTGs use a fixed length frame of 0.5-ms duration at 16 Kbps, and 0.25-ms duration at 32-Kbps voice digitization rates (VDRs). The time slot structure within the major frame is organized into either four or eight minor frames. The MSF organization using four minor frames (Type 2 MSF only) provides a primary overhead time slot structure with four traffic channels while the organization with eight minor frames provides 143 traffic channels.

C.3 Framing Sub -channel

The sequence of framing bits from each major frame is the framing sub-channel. Framing bit sequences are used to define major frames and are also used to control operation of DTG link sections between equipment. The operation is applicable all multiplex signal formats and primary overhead channelization plans.

C.4 Frame Codes

In-Sync Frame Pattern - Alternating one-zero sequence at 2/4 kb/s rate

Out-of-Sync Frame Pattern - All ones sequence at 2/4 kb/s rate

Suppressed Frame Pattern - Alternating 1100 sequence at 2/4 kb/s rate

C.5 Frame Control Signal Formats

Frame Request Signal - Out of sync frame pattern in frame bit time slot, all other multiplex frame time slots set to zeros. Places receiving equipment in a control state.

Frame Request Acknowledge - In-sync frame pattern in frame bit time slot, all other multiplex frame time slots set to zeros.

Multiplex Signal Format - Controlled response to Frame Request Acknowledge signal.

C.6 Error Recovery

The frame control convention for MSF provides the facility to resynchronize each link section independent of the synchronization state of other connecting link sections. In general, a 16/32 kb/s user-to-user circuit traverses a number of individual link sections, which make up the transmission route between the two user terminals. Loss of synchronization in any particular link section will temporarily disrupt service afforded to some users. The degradation service is more or less severe depending upon the capacity of the link and the current service demands. Some user terminals, which are affected by this disruption, may be quiescent while others may be in use.

C.7 Digital Group Multiplexer (DGM) Family

The DGM are a family of multiplexers modems cable drivers, pulse restorers and cable orderwire units compatible with the AN/TTC-39 circuit switch, AN/TSQ-111 Communications Nodal Control Element, AN/TSQ-16 Communications Systems Control Element, KY-68 Digital Subscriber Voice Terminal, KG81 Trunk Encryption Device, and TD-660, TD-754 and TD-976 multiplexers. The family includes:

A. Loop Group Multiplexer, TD-1235

B. Master Group Multiplexer, TD-1237

C. Remote Loop Group Multiplexer, TD1233

D. Remote Multiplexer Combiner, TD-1234

E. Trunk Group Multiplexer, TD-1236

C.8 Loop Group Multiplexer (LGM)

The LGM time division multiplexes 16 or 32 kb/s, four wire full duplex digital channels into a single, serialized bit interlaced group channel and also performs the reciprocal process of single group channel to individual channel demultiplexing. The LGM utilizes a Type 1 Multiplex Signal Format.

The LGM provides pre-transmission combining and post-transmission de-combining for digital voice terminal intercommunications. The LGM is the primary interface between DSVT and DDNVT Loop Modems and cable or radio link transmission equipment. The LGM is capable of accepting 7, 8, 15, and 17 32 kb/s channels with commensurate output bit rates established at 256, 288, 512 and 576 kb/s respectively. At the 16 kb/s rate, each output rate is halved.

The LGM is operationally compatible with the DSVT Loop Modem, the DNVT Loop Modem, the Trunk Group Multiplexer, the Master Group Multiplexer, the Group and Cable Driver Modems, and Trunk Encryption Devices.

C.9 Master Group Multiplexer (MGM)

The MGM is located in the AN/TSQ-111 and within the Radio Park. The MGM multiplexes up to 12 asynchronous group or super group channels in to a master group channel and provides the reciprocal demultiplexing function. Input bit rates range from 72 kb/s to 4.9152 Mb/s and the master group channel rate is either 9.36 or 18.72 Mb/s

The MGM provides two orderwire channels as part of the overhead function. The channel bit rate is 16 kb/s The MGM provides a major function of consolidating groups and supergroups at a single node for transmission to/from the radio park via a cable or short-range wide band radio link. It receives its input from the LGM, TGM, RLGM, RMC and TD-660 multiplexers.

C.10 Remote Loop Group Multiplexer (RLGM)

The RLGM time division multiplexes 16 or 32 kb/s, four wire full duplex digital loops into a single serialized, bit interlaced group channel and provides the reciprocal process of group channel to individual loop demultiplexing. The RLGM utilizes a Type 2 Multiplex Signal Format. The multiplexer is designed for unattended field use and is fully portable. It provides the interface between DSVT and DNVT subscribers and RLGM cable drivers, Remote Multiplexer Combiners or Group Modems.

C.11 Remote Multiplexer Co mbiner (RMC)

The RMC is used in exposed locations in the field. It time division multiplexes 16 or 32 kb/s four wire full duplex digital channels into a single, serialized, bit interlaced group channel and provides a demultiplexing function. The RMC utilizes a Type 1 Multiplex Signal Format. The RMC provides capacity for 7, 8, 15, or 17 channels, which may be formed by combining local loop, input channels and Type 1 or Type 2 group input channels.

C.12 Trunk Group Multiplexer (TGM)

The TGM multiplexes tow, three or four full duplex digital group channels into a single, serialized, bit interlaced supergroup channel and also performs the reciprocal process of supergroup channel to individual group channel demultiplexing. The TGM utilizes a Type 3 Multiplex Signal Format. The input group channel bit rates can range from 72 to 2304 kb/s with commensurate output supergroup channel bit rates ranging from 144 to 4608 kb/s. Output bit rates are selected in accordance with specified combinations of input group rates. The primary function of the TGM is to multiplex group output channels from the LGM, RLGM, RMC and the TD-660 Multiplexer into a single supergroup channel serving as an input to Trunk Encryption Device or a Master Group Multiplexer.

C.13 Subchanne l

A contiguous bit stream placed in or extracted from a particular time slot or set of time slots associated with an overhead channelization plan.

THIS PAGE INTENTIONALLY LEFT BLANK

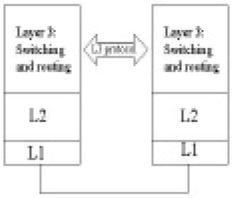
THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D (Circuit Switched Control Plane)

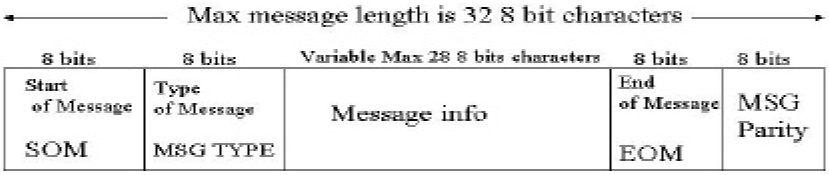
D.1 Circuit switched control plane layer 3

The circuit switched layer 3 flood search control protocol is a standard set of messages that go between the switching and routing functions of two nodes.

These messages are sent between switches to set up and negotiate switching and routing information. All messages at this layer are used for channel signaling, control and supervision of switches. The messages are then sent to a layer 2 protocol. When a call or service is requested, messages are sent between the switches using the flood search algorithm. The algorithm, although proprietary uses information sent between switches on the Routing subsystem channel to determine the best path or which node to begin sending route request messages. The flood search algorithm uses TGC or links that are connected to Large extension nodes, tandem flood search capable links based on occupancy of the trunks, delayed request routes such as satellite links. The particulars of this algorithm are a proprietary to GTE and are contained in BBN reports C 25, C28 (software GTE contracted company) and in ICD 13 and 14 (GTE interconnection documents of common signaling).



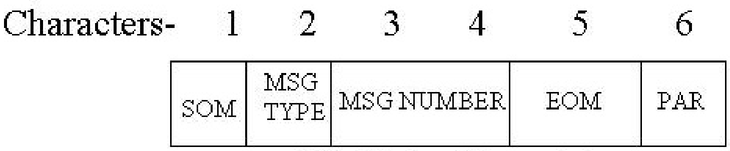
The messages are all sent down to layer 2 with the following start of message, Message type, end of message and parity check field. The SOM, EOM or 8 bit flags indicating the start or end of a message. The message type field is an 8-bit character based on message type. The Tri TAC Document TT- A3-9016-0056A dated 24 September 1992 is the Digital Common Channel Signaling/ Supervision Plan, which contains all most of the messages. All of the messages, which are considered confidential by GTE or General Dynamics, are contained in the



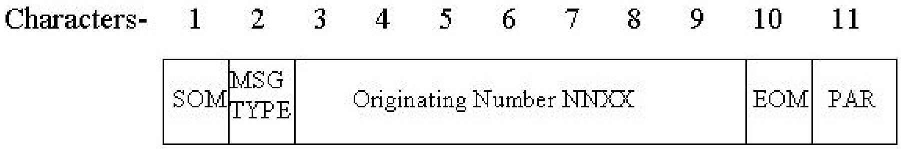
BBN reports and ICD 13 and 14, but some example message type fields are taken from PS-00-1391640C, (Addendum specification to Digital Common Channel Signaling/ Supervision Plan).

Bits	-	Message type
00001000	-	Assign essential user circuit
00001100	-	EUB Delete
00010100	-	Restore EUB
00010110	-	Bulk Transfer
00100000	-	Call Initiate for dedicated line

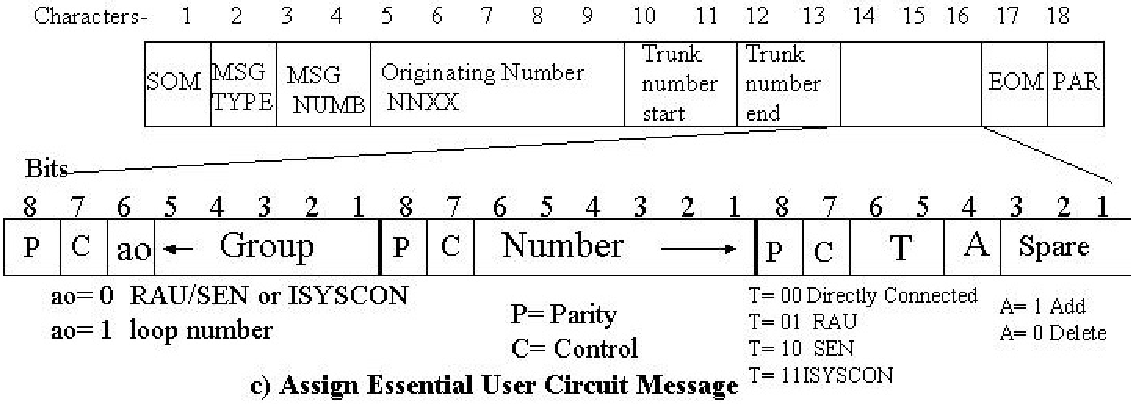
The Variable information contains information pertinent to each on the messages. The Maximum length of the entire message cannot be any more than 32 8 bit characters, or 256 bits, or when received by layer 2, will be dropped. Fields in the variable part of the message contain information pertaining to the originating address or phone number, trunk start number, trunk end number group number, connection type, and message number. Examples some messages are:



a) EUB Delete Message Format



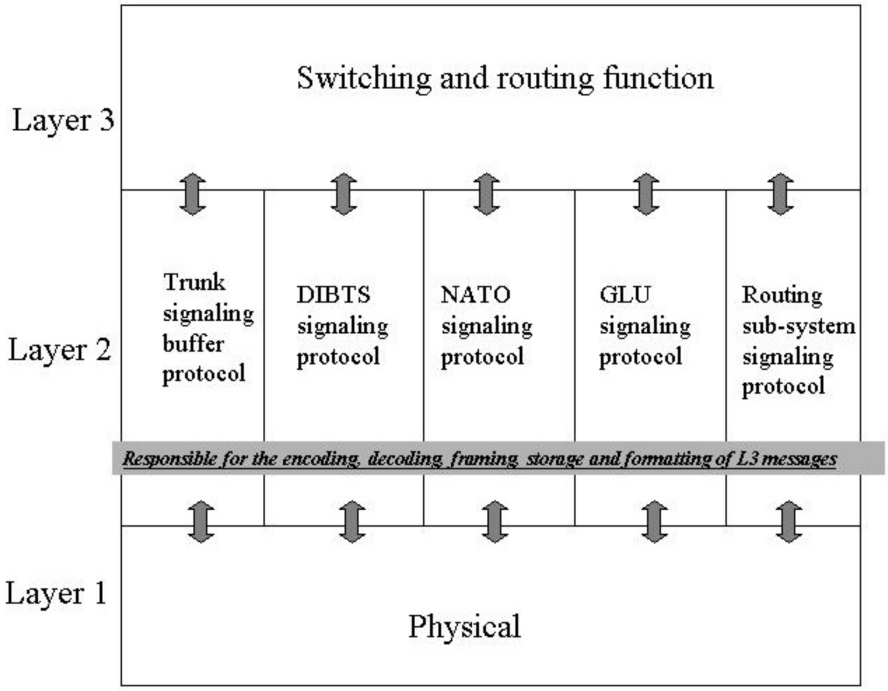
b) Restore from EUB Message Format



c) Assign Essential User Circuit Message

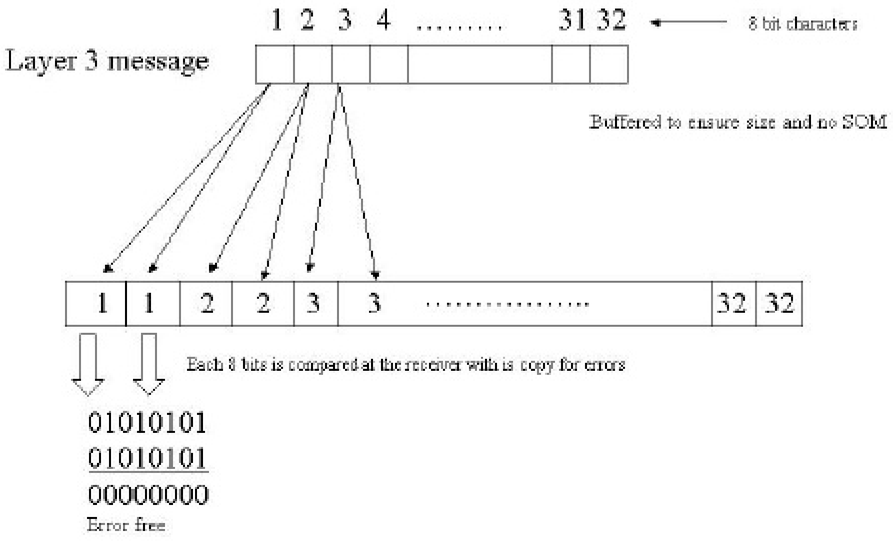
D.2 Circuit switched control plane layer 2

Messages received or destine for the layer 3 flood search routing protocol use a specific layer 2 message format. Messages for call or circuit setup use the layer 2 trunk signaling buffer (TSB) protocol, when being sent between two flood search capable switches. Layer 3 messages use the Digital-in-Band Signaling (DIBITS) Protocol between a flood search switch and a non-flood search capable switch. Layer 3 messages going to a NATO switch use the layer 2 NATO Signaling Protocol. Layer 3 messages between a switch and a RAU use the layer 2 GLU Signaling protocol. Layer 3 messages pertaining to routing updates, or request from operators such as affiliation requests use the Routing subsystem (RSS) protocol.


Layer 3
Switching and routing function
Layer 2
Trunk signaling buffer protocol
DIBTS signaling protocol
NATO signaling protocol
GLU signaling protocol
Routing sub-system signaling protocol
Responsible for the encoding, decoding, framing, storage and formatting of L3 messages
Layer 1
Physical

D.2.1 Trunk Signaling Buffer Protocol

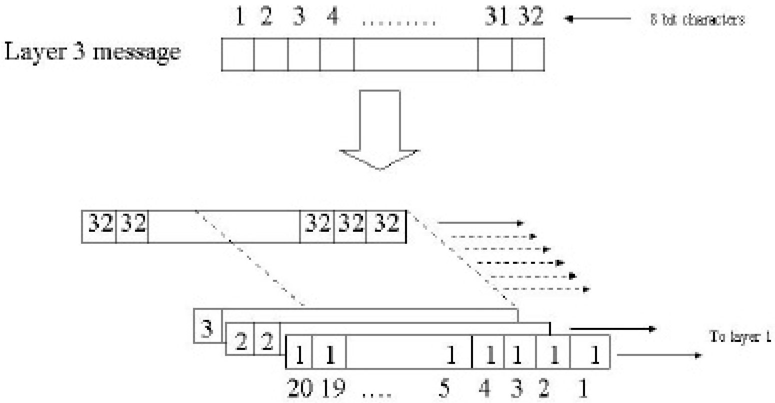
The trunk signaling buffer protocol receives messages from the L3 and encodes, formats, stores checks and sends messages to layer 1. If no messages are being received to send the Protocol sends and receives idle characters to layer 1. Synchronization is kept by monitoring the line for idle or SOM characters. Failure to receive either one within 100 characters signals resynchronization procedures. Once a message is received from L3 it is buffered and checked for proper length. If the message is greater than 32 8 bit characters or a SOM from L3 is identified, then, the message is discarded. Once the entire message is received, each 8-bit character is doubled and sent as a 16-bit character, which is used for error checking, if there is a difference is the two identical characters then an error has occurred and the message is discarded.



D.2.2 DIBITS SIGNALING PROTOCOL

The DIBITS signaling buffer protocol receives messages from the L3 and encodes, formats, stores checks and sends messages to layer 1. If no messages are being received or sent the DIBITS Protocol continually sends and detects idle characters. The DIBTS protocol receives messages from the L3 flood search routing protocol and sends 20 consecutive copies of the characters. If the receiver does not receive the EOM with-in the time it takes 60 characters, the message is terminated.

The detailed description of the DIBTS Signaling protocol can be found in the ICD 13 and 14, which are the common channel signaling protocols.



D.2.3 NATO SIGNALING PROTOCOL

The NATO Signaling protocol works in two modes satellite or terrestrial. The NATO Signaling Protocol performs error detection, encoding, decoding an overall parity check, handshaking, synchronization and retransmission on request. The terrestrial mode requires block-by-block acknowledgement scheme without a message-by-message acknowledgement scheme. The request retransmission is used when a block in error.

Layer 3 messages are formatted into 32 bit words. When a complete message is received and synchronization is maintained (Both sides are transmitting or receiving Sync messages) the message is processed and transmitted in blocks.

Once a message is received and broken into blocks, the block is encapsulated with a block header, OK/RO bit, forward error detection and overall parity. The blocks are then sent to layer 1 with no gaps. The exact process is contained in the TRI TAC document TT- A3-9016-0056A.

D.2.4 ROUTING SUB -SYSTEM PROTOCOL

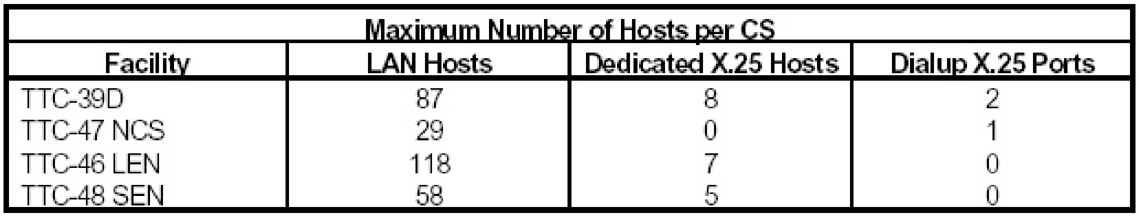
This protocol is used to transfer messages to and from the switch and requests from messages pertaining to information contained in the routing sub-system data-base, such as affiliation, black listing and profile information. If the switching or routing sub-system needs some information about another switch, such as affiliation or black listing, the processor has the layer 3 protocol send a message asking for this information, which is sent down the layer 2 RSS signaling protocol to the other switch. The detailed information about the routing sub-system is a proprietary document ICD-13 and ICD-14. ICD-13 and 14 are General Dynamic's documents, which the contract specified the Army would not receive. Difference between the RSS channel and the TSB channel, is the TSB is associated with call supervision, while the RSS channel handles routing and information transfer.

D.2.5 GLU SIGNALING PROTOCOL

The MSE Radio Access Unit (RAU) uses a Group logic unit (GLU) to function as an access device for mobile subscribers into the MSE network. The GLU physical layer or layer 1 is a 16 kbps channel associated with the RAU Digital Transmission Group (DTG). This Channel is used for control and signaling associated with affiliation, frequency plan transfer from the SCC or to Mobile subscriber terminals. The GLU can either operate in a data mode or a voice mode. The data mode is for frequency plan transfer from the SCC and the voice mode is for frequency plan distribution to a mobile subscriber. **The GLU Signaling protocol** is used for the layer 2 function of the transfer from the node center to the GLU. This information is sent from the SCC to the NC switching and routing layer and then to the GLU via the GLU signaling protocol. This Protocol is used by the flood search routing protocol, which sends messages to the GLU Signaling Protocol and then down to layer 1. This is described in the proprietary SR-14. The GLU signaling protocol must perform the following functions as a layer 2 protocol; Encoding, decoding, framing, error checking or correction. All other functions such as GLU affiliation, disaffiliation, subscriber affiliation, voice calls are done using the in-channel terminal to switch protocol described in the circuit switch voice layer 2 protocol. In the case of a RAU, the GLU is a terminal or user device, which acts as a special terminal to give mobile subscribers access to the network via a direct channel. No detailed information about what this layer 2 protocol does could be found, but it must do framing, encoding, decoding and some type of error control.

Appendix E (MPN UNI and NNI Plane Supplement)

Within a given network there can be a maximum of 1250 hosts interfacing to the TPN as X.25 or IEEE 802.3/Ethernet 2 Local Area Network (LAN) subscribers. Additionally, the TPN provides an electronic mail capability and allows up to 1200 mail recipients in a network to register at any host to receive mail. The following table summarizes the maximum number of user hosts by type that can interface with the MSE system.



Maximum Number of Hosts per CS			
Facility	LAN Hosts	Dedicated X.25 Hosts	Dialup X.25 Ports
TTC-39D	87	8	2
TTC-47 NCS	29	0	1
TTC-46 LEN	118	7	0
TTC-48 SEN	58	5	0

Table 3-7: Maximum Number of Hosts per CS

E.1 LAN Hosts User to Network Interface

The IGW serves as a RARP server as mentioned in paragraph 4.3.1. The IGW also uses Proxy ARP, which is virtually the same as an ARP request. When a host user requests the IP address of a host that is within the LAN segment connected to the IGW, it returns its own physical address. This allows traffic to be routed to an off-LAN host can be sent to the IGW for subsequent routing to the MPN backbone.[29]

MPN hosts accept IP packets up to 576 bytes, which includes the header, without fragmentation. Datagrams sent to the IGW destined for the MPN larger than 1007 bytes will be fragmented by the IGW. [30] This is to ensure that IP datagrams destined to an AHIP host will be able to be segmented into X.25 complete packet sequences.

E.2 X.25 Host User to Network Interface

In regards to flow and error control, LAN hosts and Standard X.25 hosts utilize TCP transport layer 4 protocol. X.25 hosts, basic and standard, provide end-to-end acknowledge of packets through layer 2 information (I) and supervisory (S) frames. When X.25 hosts access the MPN via dial-up over the circuit switched network (see Figure 4.3.9, Tab 1), users have the option of Forward Error Correction (FEC) when using the MDID. The MDID allows X.25 host users to select FEC during data transfer, where the 16Kbps data rate is reduced to 8Kbps, for the half-rate hamming code used in the FEC.

Additionally, MPN X.25 host users are allowed variations on X.25 standard services and are offered services not defined by the X.25 standard. At the data link LAP-B layer, MPN only supports modulo 8, not modulo 128. The greatest length of user data that the MPN allows in data packets is 1024 octets, with a standard maximum of 128 octets. This augments the restriction of X.25 hosts (Data Terminal Equipment /DTE) that use IP to select a maximum frame size that either allows IP datagrams to be transmitted in a single packet or transmits them in complete X.25 packet sequences. This restriction is imposed so that user data will fit within AHIP/1822 messages, which allows IP to be mapped over X.25. The AHIP/1822 message length is designed to accommodate an IP datagram sent as a complete packet sequence. [31]

MPN offers the following optional user facilities: 1) Non-standard Default Packet Sizes, where all DTEs (X.25 hosts) connected to a DCE (communications modem inside the PS) are using the non-standard packet size; 2) Non-standard Default Window Sizes with the same stipulation in the above facility; 3) Flow Control Parameter Negotiation ; 4) Closed User Group-Related Facilities; 5) Fast Select for Basic X.25 hosts; and 6) Hunt Group. For a more detail description, reference SR-43B.

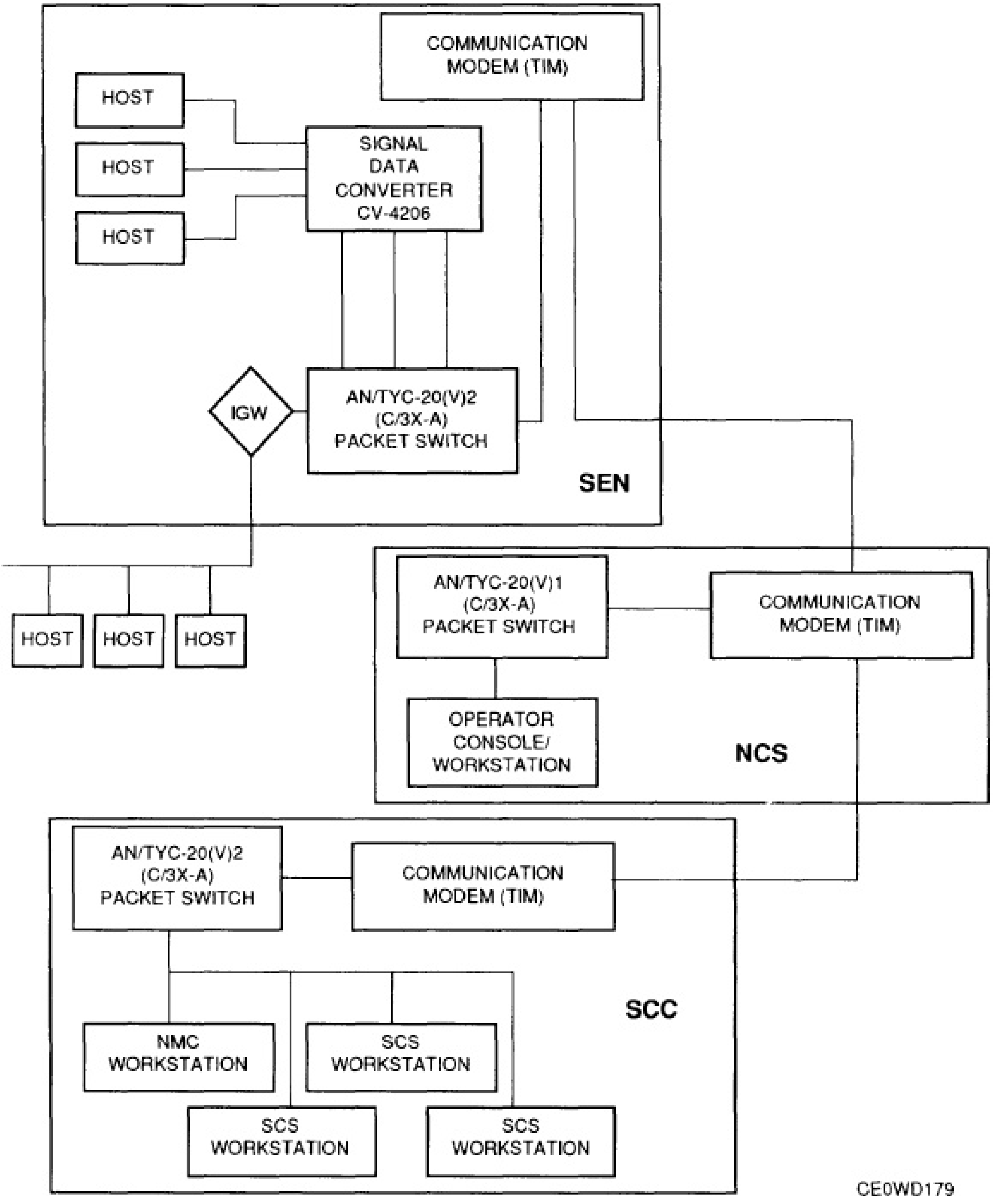
As for the non-standard X.25 services, the MPN offers 5 private user facilities. The Type of Service facility allows a X.25 user to convey to the destined end what type of X.25 service it is requesting. The Call Precedence Facility allows authorized DTEs to negotiate precedence levels for calls. There are 4 possible levels of precedence. For Standard X.25 hosts, these X.25 precedence codes are mapped to IP TOS codes thru the use of the AHIP/1822 protocol.

X.25 Code	IP Code
00	000
01	001
10	010
11	011-111

The Communities of Interest facility permits the grouping of DTEs for access purposes. Each DTE must be assigned to one COI and can belong up to 27 COIs. Logical Addressing facility allows for the accessing a DTE by a name that is independent of the device' s physical location. The NETID (Network Identifier) facility allows DTEs to determine which X.25 network they are connected.[32]

Tab 1 (MPN Diagrams) to Appendix E (MPN UNI and NNI Plane)

Figure 4.3.1 MPN Packet Switching Equipment


COMMUNICATION MODEM (TIM)
HOST
HOST
HOST
SIGNAL DATA CONVERTER CV-4206
IGW
AN/TYC-20(V)2 (C/3X-A) PACKET SWITCH
SEN
HOST
HOST
HOST
AN/TYC-20(V)1 (C/3X-A) PACKET SWITCH
COMMUNICATION MODEM (TIM)
OPERATOR CONSOLE/ WORKSTATION
NCS
AN/TYC-20(V)2 (C/3X-A) PACKET SWITCH
COMMUNICATION MODEM (TIM)
SCC
NMC WORKSTATION
SCS WORKSTATION
SCS WORKSTATION
SCS WORKSTATION
CE0WD179

Tab 1 (MPN Diagrams) to Appendix E (MPN UNI and NNI Plane)

Figure 4.3.2 MPN Access Interfaces at the NC

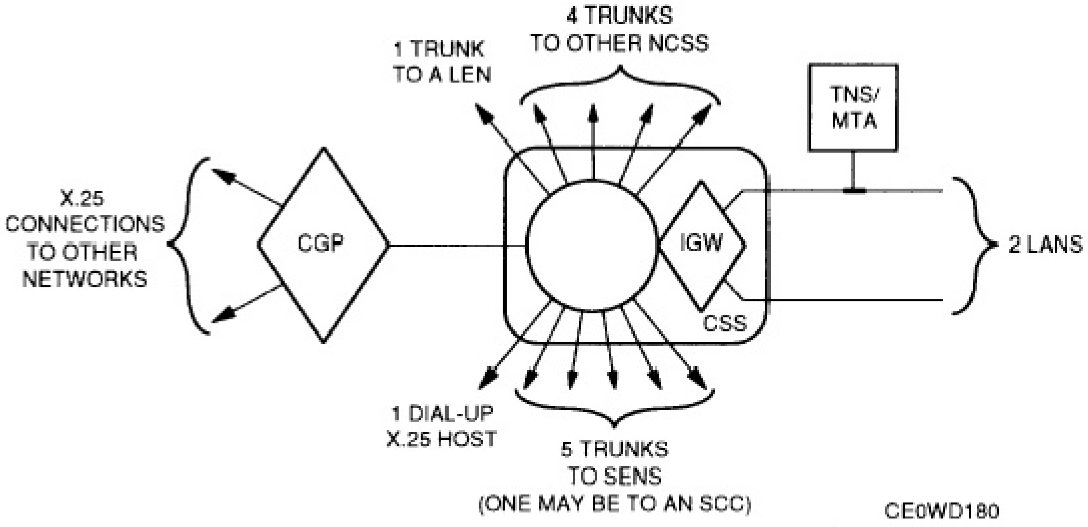
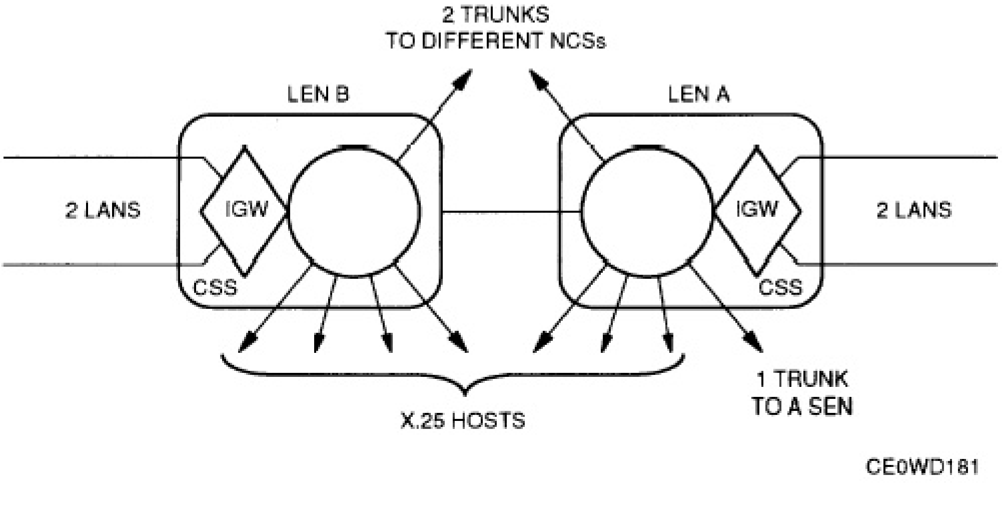


Figure 4.3.3 MPN Access Interfaces at the LEN



Tab 1 (MPN Diagrams) to Appendix E (MPN UNI and NNI Plane)

Figure 4.3.4 MPN Interfaces at the SEN

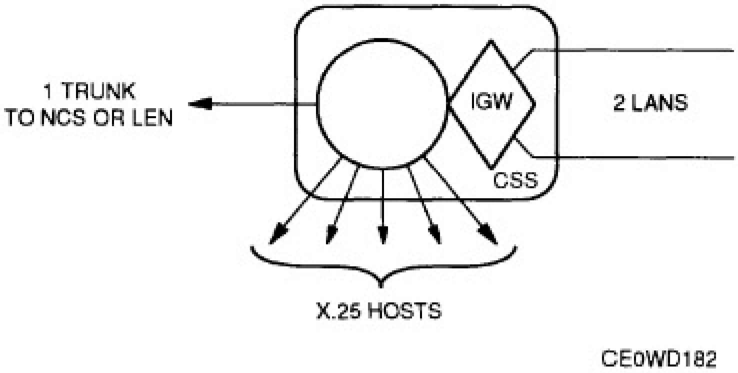
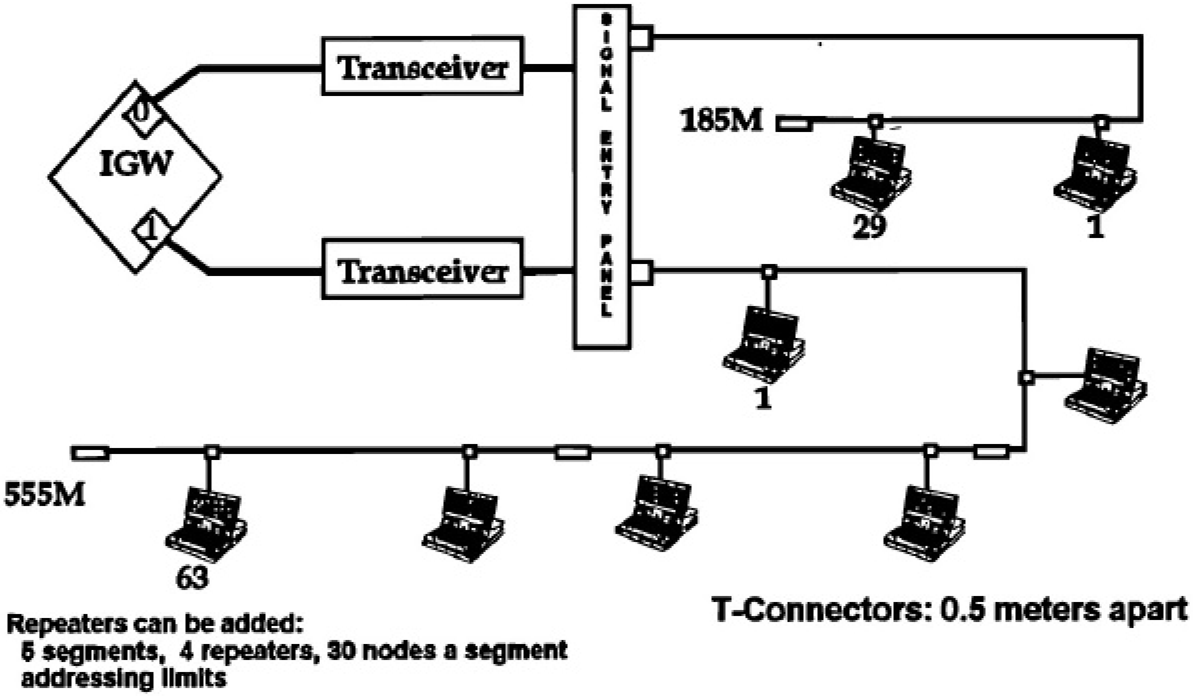
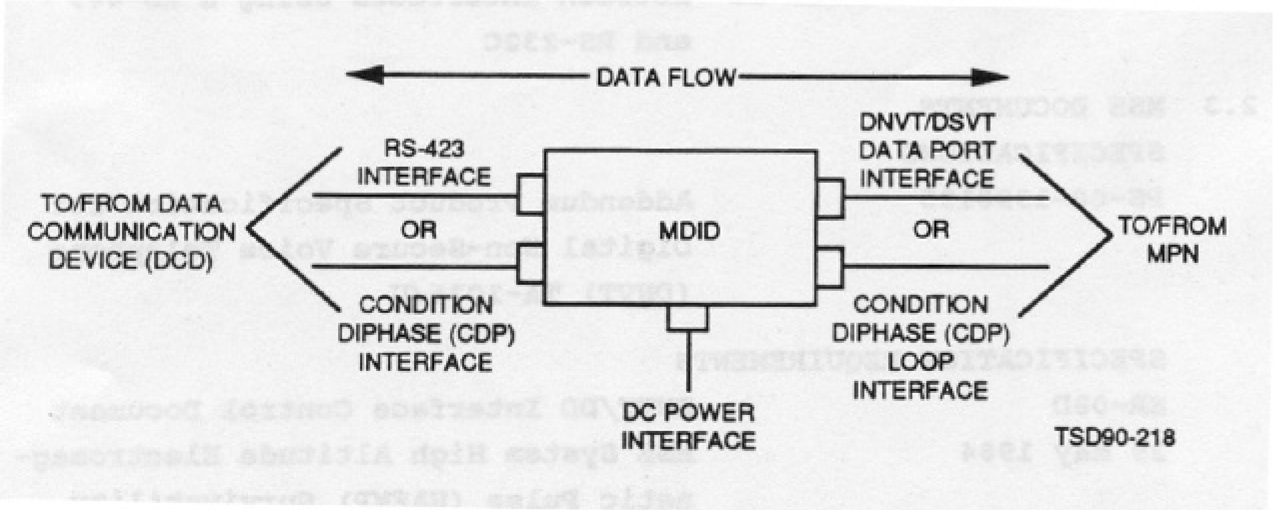


Figure 4.3.5 MPN Integral Gateway



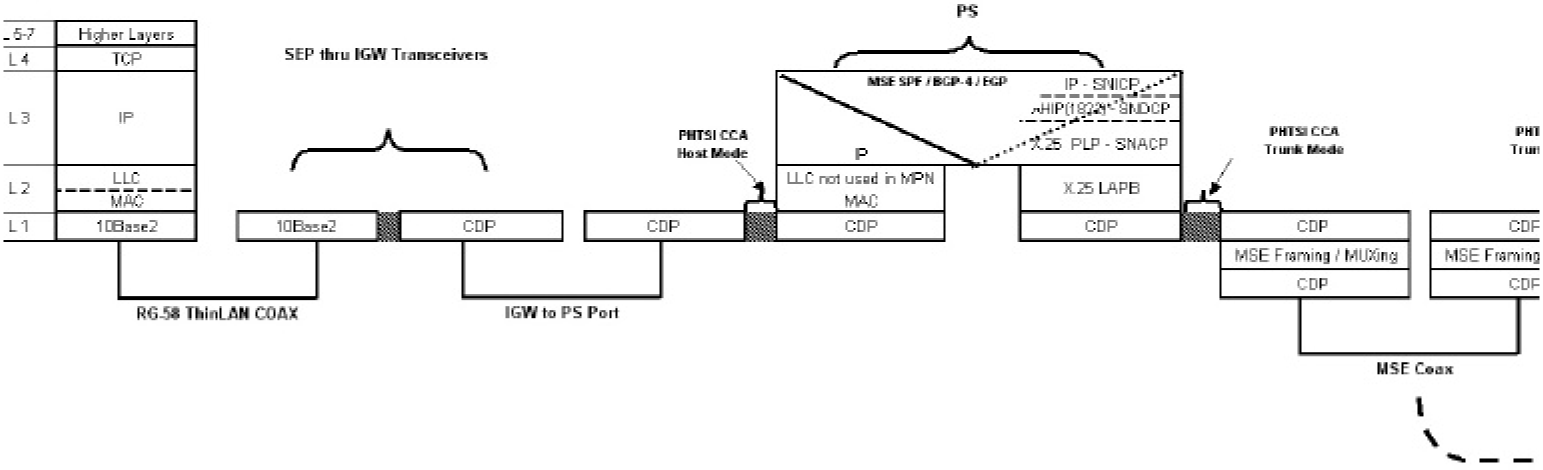
Tab 1 (MPN Diagrams) to Appendix E (MPN UNI and NNI Plane)

Figure 4.3.6 MDID Interfaces for Dial -Up Service with DNVT/DSVT



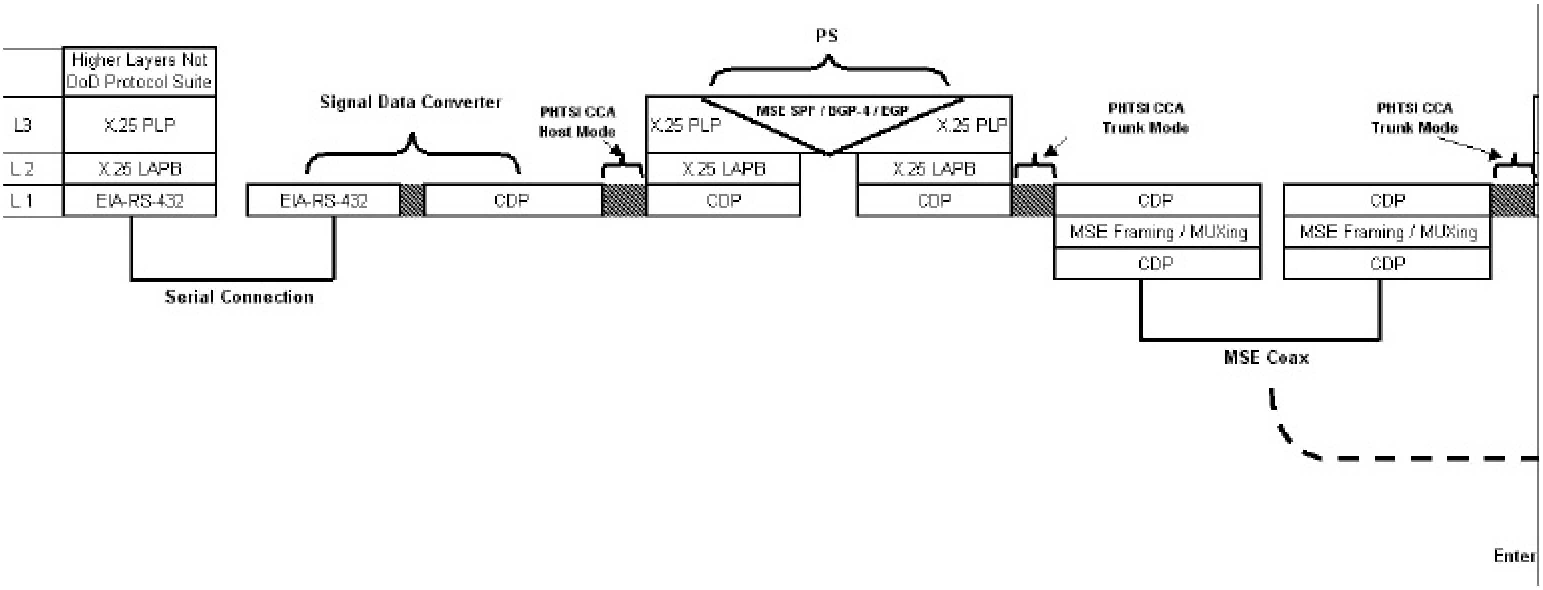
Tab 1 (MPN Diagrams) to Appendix E (MPN UNI and NNI Plane)

Figure 4.3.7 (LAN to X.25 WAN UNI Ro uting Diagram)



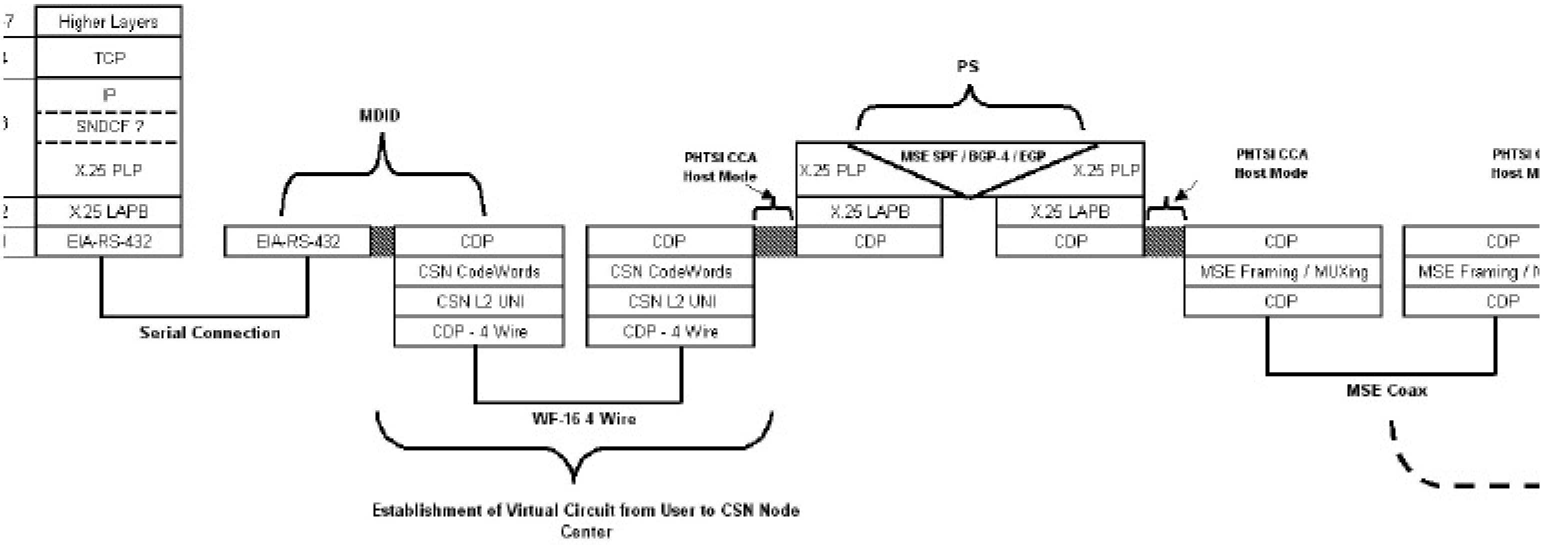
Tab 1 (MPN Diagrams) to Appendix E (MPN UNI and NNI Plane)

Figure 4.3.8 (Basic X.25 Host to X.25 WAN UNI Routing Diagram)



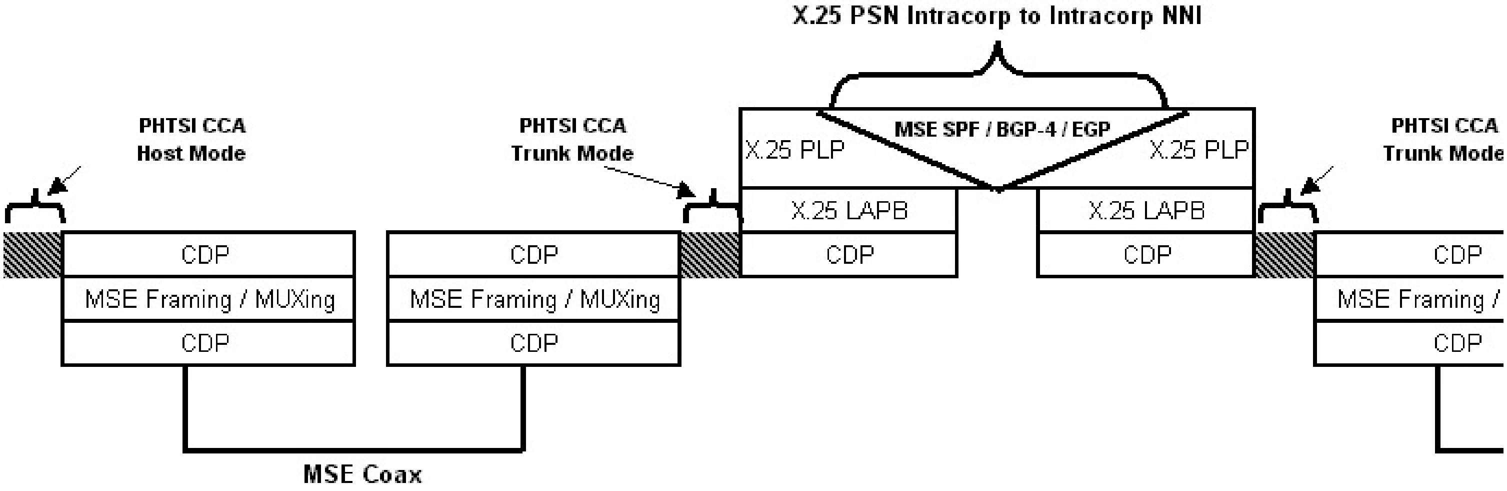
Tab 1 (MPN Diagrams) to Appendix E (MPN UNI and NNI Plane)

Figure 4.3.9 (Standard X.25 Host to X.25 WAN Dial -Up UNI Routing Diagram)



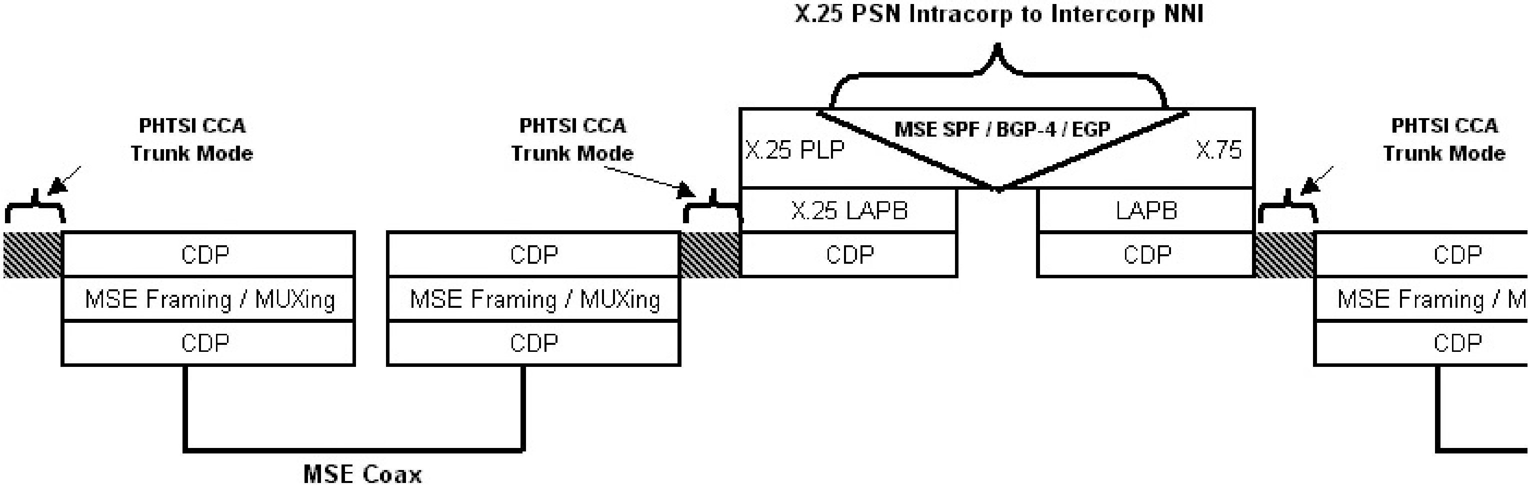
Tab 1 (MPN Diagrams) to Appendix E (MPN UNI and NNI Plane)

Figure 4.3.10 X.25 PSN Intracorp to Intracorp NNI



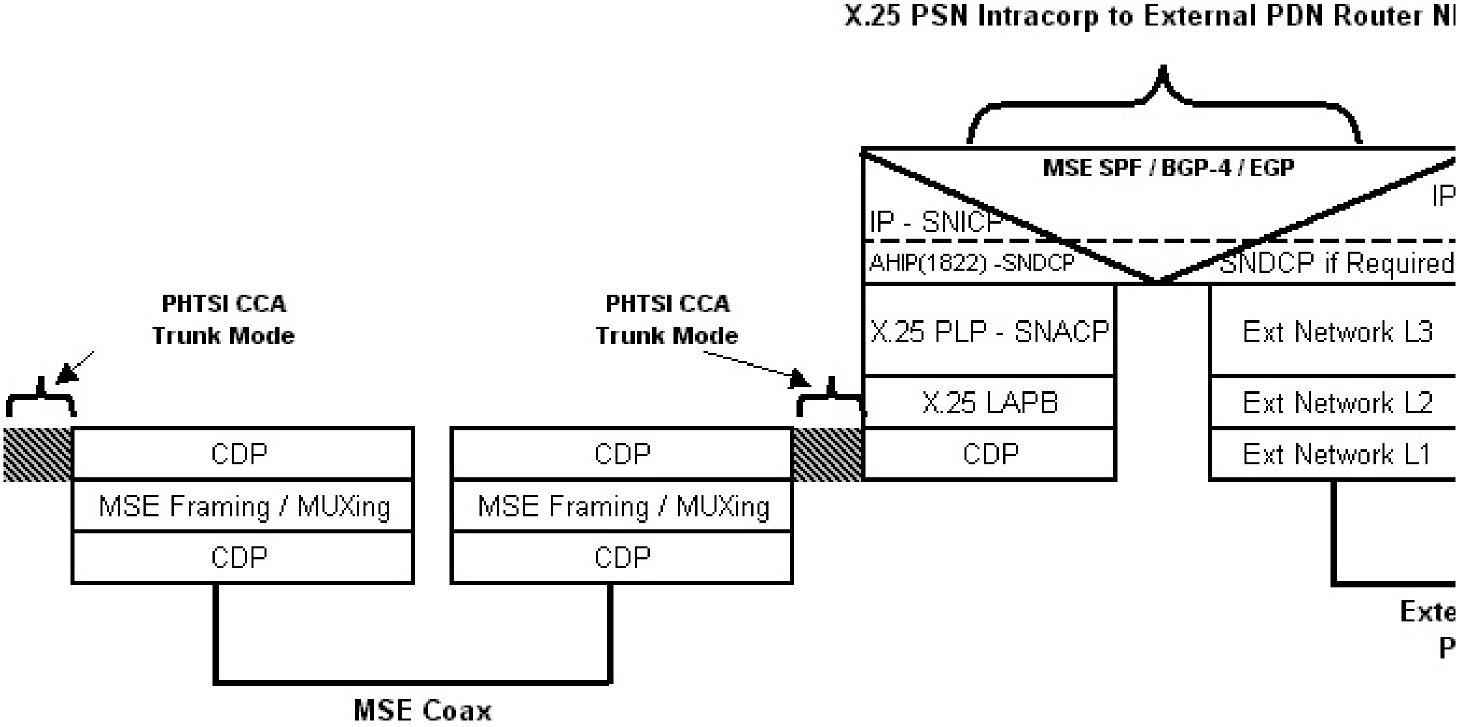
Tab 1 (MPN Diagrams) to Appendix E (MPN UNI and NNI Plane)

Figure 4.3.11 X.25 PSN Intracorp to Intercorp NNI



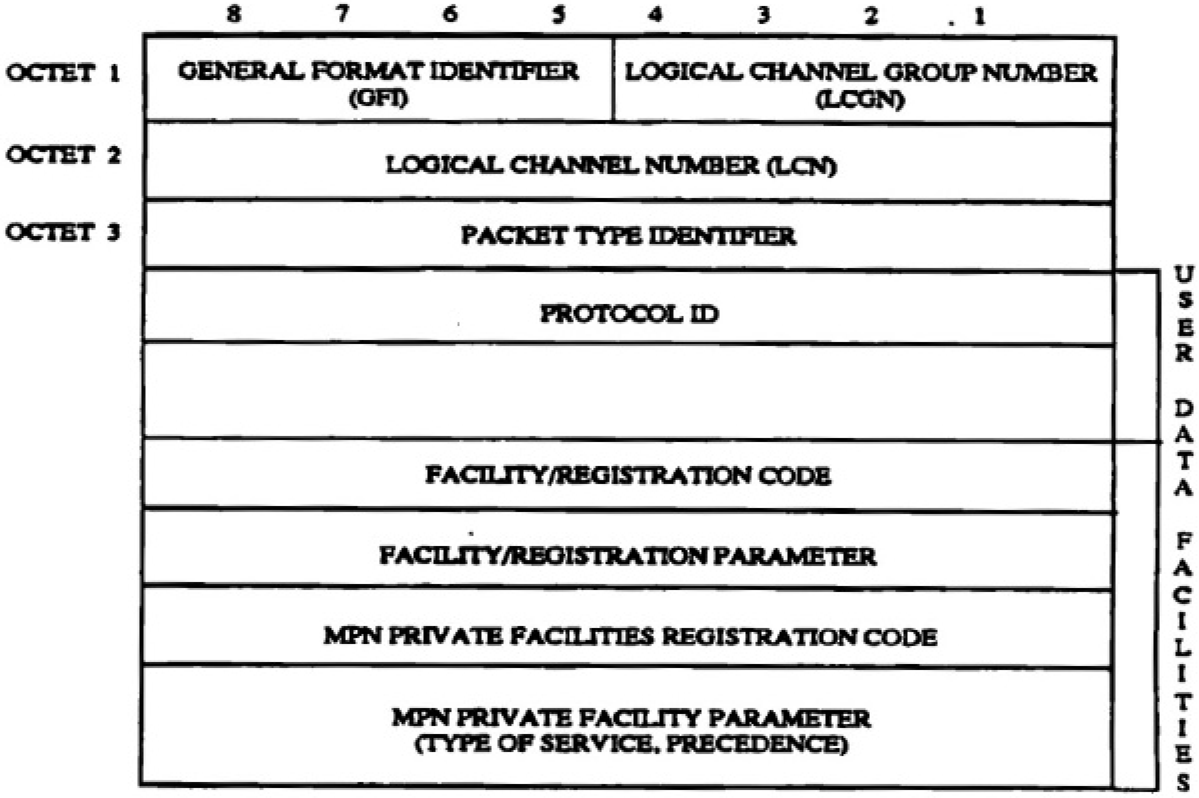
Tab 1 (MPN Diagrams) to Appendix E (MPN UNI and NNI Plane)

Figure 4.3.12 X.25 PSN Intracorp to External PDN Router NNI



Tab 1 (MPN Diagrams) to Appendix E (MPN UNI and NNI Plane)

Figure 4.3.13 MPN X.25 Packet Format


8 7 6 5 4 3 2 . 1
OCTET 1
GENERAL FORMAT IDENTIFIER (GFI)
LOGICAL CHANNEL GROUP NUMBER (LCGN)
OCTET 2
LOGICAL CHANNEL NUMBER (LCN)
OCTET 3
PACKET TYPE IDENTIFIER
PROTOCOL ID
FACILITY/REGISTRATION CODE
FACILITY/REGISTRATION PARAMETER
MPN PRIVATE FACILITIES REGISTRATION CODE
MPN PRIVATE FACILITY PARAMETER (TYPE OF SERVICE, PRECEDENCE)
USER DATA
FACILITIES

APPENDIX F (MPN NNI USER AND CONTROL PLANE)

F.1 MPN Implementation of IT U-T X.25 Control Frame's

MPN conforms to the majority of supervisory, information and unnumbered frame formats and protocols specified in ITU-T' s X.25 Standard in regards to call setup, data transfer and call termination. Two of the major differences are the different implementation of the Delivery bit (D-bit) and the SNDCP protocol AHIP/1822 that allows connectionless IP service to be encapsulated by connection oriented X.25 service. IETF RFC 877 and 979 describe AHIP/1822.

At the Layer 3 PLP, the MPN varies the delivery D-bit procedure as defined in the X.25 standard. MPN supports remote, but not local acknowledgement. It treats all packets as though the D-bit were set to 1, providing end-to-end acknowledgement only for these packets.[33] The D-bit passes through the sub-network transparently. Additionally, RFC 979 allows more efficient end-to-end functionality through a Duplex peer protocol, reducing overhead by having acknowledgement messages ride back on reverse traffic. The RFC also allows an adjustable window facility, allowing larger data fields in each IP datagram.[34]

F.2 MPN Connectionless IP Over Connected Oriented X.25

The MPN allows up to a maximum of 1024 octets of user data in the data packets with the default standard of 128 octets. Any host that communicates with another host that uses AHIP must restrict the user data bits to a maximum of 1007 octets to ensure that the user data will fit into the receivers AHIP message format. This is designed to accommodate an IP datagram sent as a complete packet sequence. [35]

Hosts that implement IP as the transport protocol must select a maximum frame size that either allows IP datagrams to be transmitted in a single packet or transmits them in complete X.25 sequences using the M-bit in the X.25 header.[36]

During a call request, the Call User Data Field contains a Protocol ID, which designates, if any, transport Layer 4 protocol it is using. If the host is using Standard X.25 service, the field will contain an ID (11001100) signifying TCP. The modem or Data Call Terminating Equipment (DCE) translates the code into an AHIP link number.[37] (See Figures 4.3.10-11, Tab 1, Appendix E)

THIS PAGE INTENTIONALLY LEFT BLANK

THIS PAGE INTENTIONAL LY LEFT BLANK

Appendix G (Security Plane)

Appendix G (Security Plane)

G.1 Call Security.

The NC switch provides the capability to classmark secure subscriber terminals as security required, security preferred, or end-to-end encryption required. A security required call can be initiated using an approved digital loop or DSVT by keying prefix digits 1C, preceded by a precedence code if desired. The call is completed only if the called subscriber is also an approved digital loop or DSVT, and a secure path is available between them. Otherwise, the call is released and error tone returned to the calling subscriber. When a security-preferred subscriber initiates a call, it is extended as a secure call if possible. If it cannot be extended as a secure call, it is extended as a non-secure call. Non-secure Warning Tone (NSWT) is sent to any subscriber classmarked for secure operation whenever that subscriber is involved in a non-secure connection. A DSVT subscriber can initiate an end-to-end encrypted call to another DSVT subscriber by keying prefix digits 4C, preceded by a precedence code, if desired.

G.2 Communication Security Equipment.

The COMSEC equipment configuration includes 15 TEDs and one TUNA housing eight dual LKGs and one AKDC. The LKG provides crypto synchronization with a variety of terminal equipment (e.g. Digital Subscriber Voice Terminal (DSVT), DNVT, and a number of EAC interfaces). Under switch control or manual operation, the LKGs accomplish synchronization, resynchronization, and key transfers necessary to operate and process end-to-end encrypted digital traffic. The TEDs are full-duplex, synchronous devices used to provide DTG bulk encryption and decryption. The cryptokey is manually loaded using an electronic transfer device. The AKDC unit interfaces with the TEDs and the LKGs and provides automatic key generation, distribution and storage for the NC switch.

G.2.1 Trunk Security

The TED (a full-duplex, synchronous device used to provide DTG bulk encryption and decryption) is used throughout the MSE system where LOS links are employed. The TEDs utilize one key: T. The T keys are divided into four groups – T_I, T_E, T_N, and T_G.

1. T_I (TED Initialization) TEK held for all NCs and LENs. Generated at the PNCS by the BCOR and pre-positioned for initial synchronization of TEDs between NCs and LENs to allow bulk transfer of TN keys over the pre-positioned Bulk Transfer (BT) key.

2. T_E (TED Extension). TEK used to secure extension links to LENs, RAUs, SENs and LOS(V)2s. Te keys are generated at the PNCS by the BCOR and pre-positioned. There is a separate Te key for each battalion. As SENs and RAUs move in support of maneuver units the gaining NC will conform to the original T_E key for that SEN or RAU.

3. T_N (TED nodal). TEK key used for intra- and inter-Node Switch Group (NSG) links.
A separate Tn key is generated for each link, by the NC designated as master. T_N keys
are updated daily by link masters

4. T_G (TED gateway). TEK used for links to adjacent Corps or Echelon Above Corps
(EAC) links. T_G keys are updated daily by link masters.

G.2.3 Orderwire Security

The Communications Security Equipment KY-57 provides the COMSEC function for the Orderwire providing secure half-duplex communications over radio and cable links. The KY-57 is installed in the NC switch, Large Extension Nodes (LENs), Small Extension Nodes (SENs), RAU assemblages, and all LOS assemblages. The KY-57 provides two capabilities, encryption of voice communications between operational personnel to provide engineering of the network, and electronic transfer of key from the NC to SEN, RAU, or LOS(V)2 NATO Interface Terminal (NIT) teams, using the Net Control Device (NCD), KYX-15. The keys contained in the KY-57 are electronically stored by the parent NC switch. Two keys are used, one for voice traffic and the other for rekey.

1. N Key. TEK used to provide protection for confidential DVOW communications between MSE teams.

2. K key. KEK generated at the PNCS by the BCOR and pre-positioned with NCs, LENs SENs and RAUs corps-wide. Used at the discretion of the BCOR for OTAR between MSE teams.

G.2.4 Switch Security

The COMSEC switch functions are implemented using the Automatic Key Distribution Centers (AKDC) or KGX-93A and the LKGs (KG-112) to provide key generation and transfer, and secure communications between subscribers or between NC switches and LEN switches. The switch uses three basic keys to communicate:

1. CIRK (Common Inter-switch Re-Key). Network common KEK used to encrypt the transmission of the per call key between NCs/LENs.

2. CBTV (Common Bulk Transfer Variable). KEK used to encrypt the bulk transfer of keys from the Hardened Unique Storage (HUS) device, KGX-93A to KGX-93A between NCs/LENs.

3. AIRK (Area Inter-switch Re-key). KEK used to encrypt the transmission of the per call key across a gateway.

G.2.5 Subscriber Security

Encrypted subscriber traffic/functions are implemented by the MSRT, which consists of a DSVT and a RT-1539A (RT-1539). Both the DSVT and the RT-1539 contain key generators that provide secure communication (using the U and M key). For a cold start, the subscriber is provided keys that are loaded into the MSRT with the electronic transfer device (KYK-13). Direct MSRT-to-MSRT communication is approved on an exception basis only. The MSRT automatically affiliates with the network once the keys have been properly loaded and the subscriber has initiated the affiliation process. Additional keys used in subscriber security are:

1. X Key (DSVT Net Key). TEK used to encrypt synchronization signaling between the NC/LEN and the DSVT or KY-90.

2. V Key (Per call Key). TEK automatically generates and sends to the DSVT or KY-90 as part of the call setup procedure.

3. MSRV (Message Switch Rekey Variable). KEK is used to encrypt transmissions of the per call key to the TYC-39 Message Switch.

4. MSNV (Message Switch Net Key). TEK used to encrypt the synchronization signaling over MSRT, NRI (KY-90) and TS/SCI users.

5. M Key. TEK used to encrypt signaling between the MSRT and RAU. Also used to provide DSVT subscribers initial entry into the network by encrypting the synchronization signaling between the NC/LEN/FES and the DSVT.

6. U Key. KEK used to encrypt the transmission of per call and X keys between NC/LEN and the DSVT or KY-90. Subscribers are assigned to one of twenty-five U keys based on their profile.

7. S Key. Compartmental TEK used in the DSVT by a small community of users to protect highly classified information. The S key must come from a paper tape canister or be generated by a TS certified KG-83. It is loaded into the KY-68 by the user at each end, after first completing a call to the distant end. It overwrites the current U key and is good for the length of the call, and then it must be reloaded for the next special call. The S key is not an MSE key; it is a user provided key.

To enable communications through interface with the Single Channel Ground and Airborne Radio Systems (SINCGARS), a Combat Net Radio (CNR) interface unit is provided in designated SEN and LEN switches. The Secure Digital Net Radio Interface Unit (SDNRIU) KY-90 provides the capability to accommodate a variety of single channel radios. The KY-90 provides semi-automatic, half-duplex communication between single channel radio users and the MSE subscribers. The KY-90 uses an M and U key plus a CNR key.

G.3 NETWORK KEY DISTRIBUTION

Distribution of keys within the MSE network use a combination of three techniques:

1. Electronically through Bulk Transfer (BT), where bulk transfer is the transfer of keys from one KGX-93, AKDC to another KGX-93, AKDC.

2. Electronically by the DVOW, via OTAR transfer using the Manual Key (MK) of the DVOW.

3. Physically using an electronic transfer device (KGK-12/16, KYX-15, KYK-13 or CYZ-10).

G.3.1 PRE -POSITIONED KEYS

Pre-positioned keys at the Node Center/FES

KEY	USE
T_I	TED
BT	Switch to Switch
N	DVOW
K	DVOW

Pre-positioned keys at the LEN

KEY	USE
T_I	TED
M	DSVT
U	DSVT
N	DVOW
K	DVOW

Pre-positioned keys at the SEN

KEY	USE
T_E	TED
N	DVOW
K	DVOW
U	KY-90
M	KY-90
CNV	CNRI

Pre-positioned keys at the RAU

KEY	USE
T_I	TED
M	MSRT/DSVT
U	DSVT
N	DVOW
K	DVOW

Pre-positioned keys at the TRC-190 V2 NAI

KEY	USE
T_G	TED
N	DVOW
K	DVOW

Pre-positioned keys at the TRC -190 V1, 3, and 4

KEY	USE
N	DVOW
K	DVOW

Pre-positioned keys for the subscriber

KEY	USE
M	DSVT/MSRT
U(1-25)	DSVT

Table G.3.1 shows the allocation and normal source required keys for a Common-Based Circuit Switch operating in a network:

KEY	PURPOSE	ALLOCATION	NORMAL SOURCE
Z	AKDC Storage Key	1 per switch	Electronic
M	MSRT/RAU/Rehome key	1 per network	IC3S
X NET	DSVT Net Key	1 per switch	Electronic
U NETS (1-25)	DSVT U Net Key # 1-25	1 set of 25 per network	IC3S
CIRK	Common Interswitch Rekey Key	1 for Home Area Code	IC3S
AIRK	Area Interswitch Rekey Key	1 per Foreign Area Code	IC3S
T_I	TED (Interswitch)	1 per network	IC3S
T_E	TED (Extension)	1 per network	IC3S
CNV	Common Net Variable (DVOW Key)	1 per network	IC3S
BT	Bulk Transfer Key	1 per network	IC3S

G.3.2 Required keys for a Common -Based Circuit Switched Network:

1. Z key. This key is used to encrypt keys for storage in the HGX-83A or KGX-93A AKDC. This is a switch unique key, the same key should be loaded in both AKDCs, but there is no requirement for the Z key to be the same in all switches.

2. M key. This key is a combined Rehome or Re-Entry Home (RH) key and the Mobile Subscriber Radio Terminal (MSRT) key. Subscribers load the M key into their DSVT (in the "XVAR" position) and into the MSRT (if one is used). When the DSVT initially enters or re-

enters the network, the M key is overwritten with the X key. To allow subscribers to move between switches, this key must be the same across the network (within the home area code).

3. X Key. This key is automatically downloaded to the DSVT (overwriting the M key) when the subscriber enters or affiliates with a switch. All DSVTs on a given switch will share the same X key on entry. Since the X key is used for Essential User Bypass, it must be the same for all switches.

4. U Net Key 1-25. These 25 keys are the unique keys for all DSVTs. Each U Net Key can support a maximum of 150 subscribers. The specific U Net Key assigned to a subscriber is determined by profile assignment. The subscribers load their U Key into their DSVTs (In the "UVAR" position). To allow subscribers to move between switches, these keys must be the same across the network (within the home area code)

5. CIRK (Common Interswitch Rekey Key). This key is the common key used to secure the Per Call Variable transfer within the home area code. All switches within the home area code must have the same CIRK.

6. AIRK (Area Interswitch Rekey Key). This key is the common key used to secure the Per Call Variable transfer between area codes. Only Gateway switches require this key. If a single CBCS has two gateways into another network, the AIRK must be the same for all three switches.

7. T Keys (Trunk Encryption Device Traffic Keys). There are two types of T keys needed: TED Interswitch (T_I) and TED Extension (T_E) Keys.

a. The T_I key normally comes from the IC3 key matrix and is the traffic variable used to bulk encrypt a DTG between two CBCSs or between a CBCS and a TTC-39Av1 or TTC-42.

b. The T_E key is a traffic variable used to bulk encrypt a DTG between a CBCS and a SEN, SB-3865, RAU, or remote multiplexer. One T_E key is used within a network to allow re-homing of extension nodes.

8. CNV Key (Common Net Variable – Engineering Orderwire or Digital Voice Orderwire (DVOW) Key). This key is used to secure the VINSON used by the DVOW. All assemblages equipped with DVOW must share the key.

9. BT (Bulk Transfer Key), These keys are used to secure keys when transferred between CBCSs. The same variable is used to secure transfers between any switch, so the same variable is loaded in all BT locations.

Table G.3.2 shows the optional keys required to support specific applications within a CBCS network:

Optional Keys for a CBCS Network

KEY	PURPOSE	ALLOCATION	NORMAL SOURCE
S	Special Purpose (TS or SCI DSVT Calls)	1 per TS/SCI Community	Electronic
MSNV	Message Switch Net Variable	1 per CS-MS Trunk Group Cluster	Electronic
MSRV	Message Switch Rekey Variable	1 per trunk in the CS-MS Trunk Group Cluster	Electronic
HN	Home Net Variable	1 per SB-3865	Electronic
HRV	Home Rekey Variable	1 per SB-3865	Electronic

1. S Key. This key is used to provide additional security for subscribers requiring higher than SECRET level communications. Once a call is established between two DSVTs, the S key can be loaded into the "SVAR" position and provide security for the call to the classification level of the S key.

2. MSNV (Message Switch Net Variable). This key is the "X" key or Net key for trunks between a Circuit Switch (CS) and a Message Switch (MS). The same MSNV is used for al trunks in a CS-MS Trunk Group Cluster.

3. MSRV (Message Switch Rekey Variable). This is the "U" key or Rekey key for trunks between a CS and a MS. Each trunk in the Trunk Group Cluster will have a unique MSRV.

4. HN (Home Net). This is the "C" key or Net key for DSVTs supported by an SB-3865 Unit Level Circuit Switch (ULCS). The HN is common for all DSVTs on a specific SB-3865.

a. The SB-3865 is a COMSEC Subordinate Switch (CSS) and does not have an SKDC or LKGs. DSVT subscribers of the SB-3865 are provided service by a CBCS or TTC-42, acting as a COMSEC Parent Switch.

b. DSVT subscribers on a SB-3865 supported by a CBCS will load the "M" key in the "XVAR" position of their DSVT and the HRV key.

c. Once the CS to SB-3865 link is active, the CS Switch Supervisor initiates a "Cold Start" process. This identifies the nets for the SB-3865 and allows it to go to "Normal" mode.

d. The HN key is automatically downloaded into the DSVT during initial entry or re-entry of the DSVT. There is no requirement for the HN key to be the same in all SB-3865s or in all COMSEC Parent Switches.

5. HRV (Home Rekey Variable). This is the "U" key or Rekey variable for DSVTs supported by an SB-3865 ULCS. The HRV is held in common by all DSVTs assigned to a specific SB-3865.

Appendix H (MANAGEMENT)

H. Network Management

MSE uses the IMS software for Network Management. The IMS software is the GUI in front of the Network Management system. The actual Network Management is done using, ICMP, SNMP Framework with MIB1 and some type of Remote procedure calls. As outlined in the paper, the exact nature of the RPC could not be found. Although, the details of the RPC type functions could not be found there certain functions that they perform. These are the modem FEC On and Off, and the remote starts, loop backs and programming of TRAPS. The FEC ON/OFF changes the framing of the data and doubles the information and reduces the utilization in half, to achieve proper transmission of information. No other details could be found about the remote procedure calls, except the loop back that can be put in the modems themselves.

Appendix H (MANAGEMENT)

H.1 ICMP Protocol Overview

Internet Control Message Protocol (ICMP), documented in RFC 792 is a required protocol tightly integrated with IP. ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operations. Some of ICMP's functions are to: Announce network errors, such as a host or entire portion of the network being unreachable, due to some type of failure. The IMS Software uses ICMP to check to see if a packet switch or host is unreachable and then translate that information to an on screen display of the network status. Announce network congestion: When a router begins buffering too many packets, the router will tell the SNMP manager about that congestion. Assist Troubleshooting: ICMP supports an Echo function, which just sends a packet on a round--trip between two hosts. Ping a common network management tool, is based on this feature. Ping will transmit a series of packets, measuring average round--trip times and computing loss percentages. IMS software and the user can use these functions to detect hosts or routers on a network.

H.2 SNMP DESCRIPTION

H.2.1 SNMP Framework

SNMP is a frame used in network management. This Framework consists of a transport mechanism, the Structure of Management Information (SMI) and a Management Information Base (MIB). The Transport mechanism is SNMP. It is the protocol used to send Get, Get-next, Set, and Trap messages. These messages are sent in specific way uses certain criteria. The SMI defines these criteria. The manager and the agent must have the same set of rules to follow; these rules for what information is sent are with-in the MIB. The MIB is a repository of questions that can be asked. They define the question of what information is needed. The agent' s manager and agent use this information to transfer messages. With-in the IMS software, there is a specific set of MIB' s or questions used. They are the standard MIB 1. This MIB 1, has been replaced, but is still being used with-in MSE.

H.2.2 MIB 1

MIB 1 is defiend in RFC 1066. This RFC sets certain objects that can be used. Objects are items that can be managed within a device. The objects with-in MIB 1 are, System, Interfaces, Address Translation, IP, ICMP, TCP, UDP, EGP. IMS software uses SNMP and these specific MIB objects to obtain information about certain managed objects within devices. As long as a host has an agent and these MIB objects, the host can be managed. All or some of these objects can be loaded in the manager or agent, but both need them to send management information. For Instance, the manager in the IMS software uses the sysUpTime object in the MIB to determine how long the network management portion of the device has been active.

THIS PAGE LEFT INTENTIONALLY LEFT BLANK

THIS PAGE LEFT INTENTIONALLY LEFT BLANK

[1] Enslow, Philip H. Jr. Understanding Telecommunications Systems: A Systematic Examination of Systems Concepts, Functional Models, System Organization and Technology, Twelfth Edition; September, 2000
[2] ITU-T X.200, Information technology - Open Systems Interconnection - Basic Reference Model: The basic model
[3] Http://www.monmouth.army.mil/peoc3s/win-t/main/msefrme.htm 8/10/2001
[4] GTE System Specification, SS-00-1385963H, page 7.
[5] Stallings, William. SNMP, SNMPv2, SNMPv3 and RMON 1 and 2, Third Edition; New Jersey, 1999

[6] ITU-T X.200, Information technology - Open Systems Interconnection - Basic Reference Model: The basic model
[7] Appendix N (Packet Switching Network Supplement), TM 11-5800-216-10-4, pages N-1 – N-2.1
[8] Student Guide, Packet Switching (4C-F55/260-F15/D03), page 17
[9] SR43B, MPN (X.25) Serial Interface Description, pages 1-5
[10] SR45, MPN Local Area Network (LAN) Interface Control Document (ICD), pages 1-3
[11] SR43B, MPN (X.25) Serial Interface Description, pages 4-5
[12] SR45, MPN Local Area Network (LAN) Interface Control Document (ICD), pages 14-16
[13] SR45, MPN Local Area Network (LAN) Interface Control Document (ICD), pages 4-20
[14] SR43B, MPN (X.25) Serial Interface Description, pages 4-20.
[15] Ericsson Programatic Sweden, Connection Caching of Traffic Adaptive Dynamic Virtual Circuits, pages 13-14
[16] SR43B, MPN (X.25) Serial Interface Description, page 19
[17] RFC 979, PSN End-To-End Functional Specification, page 1, 8-9.
[18] SR43B, MPN (X.25) Serial Interface Description, page 2
[19] Appendix N (Packet Switching Network Supplement), TM 11-5800-216-10-4, pages N-6 – N-9.
[20] PS-00-2738975, MDID Product Specification, page 1-5.
[21] SR43B, MPN (X.25) Serial Interface Description, page 5
[22] www.protocols.com, Chapter 32, DTE to DCE Protocols in a PDN, page 641
[23] SR43B, MPN (X.25) Serial Interface Description, page 75
[24] ITU-T, X.25 Standard, pages 58-86.
[25] SR43B, MPN (X.25) Serial Interface Description, page 50-52
[26] SR43B, MPN (X.25) Serial Interface Description, page 39
[27] "The Tactical Packet Network", Army Communicator draft article, SIGCEN-DCD, page 3
[28] Stallings, William. SNMP, SNMPv2, SNMPv3 and RMON 1 and 2, Third Edition; New Jersey, 1999
[29] SR43B, MPN (X.25) Serial Interface Description, page 15
[30] SR43B, MPN (X.25) Serial Interface Description, page 11
[31] SR43B, MPN (X.25) Serial Interface Description, pages 9-20
[32] SR43B, MPN (X.25) Serial Interface Description, pages 20-31
[33] SR43B, MPN (X.25) Serial Interface Description, pages 28, 36
[34] ITU-T, RFC 979, pages 1-9
[35] SR43B, MPN (X.25) Serial Interface Description, page 19-20
[36] SR43B, MPN (X.25) Serial Interface Description, page 13
[37] SR43B, MPN (X.25) Serial Interface Description, page 19

References:

[1] Chairman of the Joint Chiefs of Staff Manual. (11 September 1995). Manual for Employing Joint Tactical Communications (CJCSM 6231.02). Joint Staff, Washington, DC: U.S. Government Printing Office.

[2] Chairman of the Joint Chiefs of Staff Manual. (29 February 2000). Manual for Employing Joint Tactical Communications (CJCSM 6231.04A), Joint Transmission Systems. Joint Staff, Washington, DC: U.S. Government Printing Office.

[3] Department of the Army, Interface Control Document –003, Change 5 (15 June 1982), Framing and Synchronization Protocols, GTE Government Systems Corporation, MSE Division, Taunton MA.

[4] Department of the Army, Product Specification for Communications Central (K022207), (15 December 1997), GTE Government Systems Corporation, MSE Division, Taunton MA.

[5] Department of the Army, Product Specification for Management Facility AN/TSQ-154 (PS-00-1390230B), (23 August 1988) GTE Government Systems Corporation, MSE Division, Taunton MA.

[6] Department of the Army, Product Specification for MSE Data Interface Device (MDID), (30 October 1990), GTE Government Systems Corporation, MSE Division, Taunton MA.

[7] Department of the Army. (1 November 1992). Appendix N, Packet Switching Network supplement. TM 11-5800-216-4.

[8] Department of the Army. (1 September 1991). TM 11-5800-216-10-1, System Manual, Mobile Subscriber Equipment, HQ, DA Washington, DC.

[9] Department of the Army. (1 September 1991). Mobile Subscriber Equipment, System Manual, TM-11-5800-216-10-2, Change 3 (1 March 1995). Headquarters, Department of the Army, Washington, DC: U.S. Government Printing Office.

[10] Department of the Army. (14 November 1990). FM 11-55, Mobile Subscriber Equipment (MSE) operations, HQ, DA Washington, DC.

[11] Department of the Army, (10 August 2001). www.monmouth.army.mil Office of the Project Manger, Warfighter Information Network-Tactical, Fort Monmouth, NJ.

[12] Enslow, Philip H. Jr. Understanding Telecommunications Systems: A Systematic Examination of Systems Concepts, Functional Models, System Organization and Technology, Twelfth Edition; September, 2000

[13] General Dynamics. (13 August 2000). Multiple Subscriber Equipment System Specification, SS-00-1385963H. Communication Systems, Taunton, MA.

[14] General Dynamics. (15 December 1997). Product Specification for Communication Central, PS-00-2741921C. Communication Systems, Taunton, MA.

[15] General Dynamics. (23 August 1988). Product Specification for Management Facility AN/TSQ-154, PS-00-1390230B. Communication Systems, Taunton, MA.

[16] General Dynamics. (26 February 1996). MSE System Specification, Appendix SR-43, MSE Packet Network (MPN) Serial Interface Description, GTE Government Systems Corporation, MSE Division, Taunton, MA.

[17] General Dynamics. (5 January 1991). MSE System Specification, Appendix SR-45, MSE Packet Network (MPN) Local Area Network (LAN) Interface Control Document (ICD). GTE Government Systems Corporation, MSE Division, Taunton, MA.

[18] GTE. (1 November 1998). Global Circuit Switch, Quick Reference Guide (ESOP and Global Edition), Version 3.1.0. U.S. Army Communications – Electronics Command, Contract DAAB07-96-D-F308.

[19] GTE. (7 May 1998). Reference Guide for Network and Nodal Manager, (ESOP and Global Version), Version 4.0.1. U.S. Army Communications – Electronics Command, Contract DAAB07-96-D-F308.

[20] IETF RFC 1005, The ARPANET AHIP-E Host Access Protocol, Atul Khanna, Andy Mailis, May 1987.

[21] IETF RFC 1548, The Point-to-Point Protocol (PPP), December 1993

[22] IETF RFC 1598, PPP in X.25, W. Simpson Daydreamer, March 1994

[23] IETF RFC 877, Standard for the Transmission of IP Datagrams Over Public Data Networks, J.T. Knob, September 1983.

[24] IETF RFC 979 PSN End-to-End Functional Specification, Andrew G. Malis, March 1986

[25] ITU-T RFC 1536, Multi-protocol Interconnect on X.25 and ISDN in the Packet Mode, Andrew G. Malis, August 1992.

[26] ITU-T X.200, Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model, July 1994

[27] ITU-T X.25, Interface Between DTE And DCE For Terminals Operating In The Packet Mode And Connect To Public Data Networks By Dedicated Circuit, 5 Oct 96

[28] ITU-T X.300, General Principles For Interworking Between Public Networks And Between Public Networks And Other Networks For The Provision Of Data Transmission Services, 5 October 1996

[29] ITU-T X.75, Packet-Switched Signaling System Between Public Networks Providing Data Transmission Services, October 1996

[30] ITU-T X.96, Call Progress Signals In Public Data Networks, March 2000.

[31] MAJ Mike Thorne, (date unknown). "The Tactical Packet Network", Army Communicator draft article, Signal Center-DCD.

[32] Per Jomer, 1989. "Connection Caching of Traffic Adaptive Dynamic Virtual Circuits", Ericsson Programmatic Sweden.

[33] Signal Officer Basic Course, ROA. Chapter 6, MSE Tactical Packet Network (TPN), [online]. Available:http://www.gordon.army.mil/roa/course/sobc/sop/chap6.thm, (13 August 2001).

[34] Stallings, William. Data and Computer Communications, Sixth Edition; New Jersey, 2000

[35] Stallings, William. ISDN and Broadband ISDN with Frame Relay and ATM, Fourth Edition; New Jersey, 1999

[36] Stallings, William. SNMP, SNMPv2, SNMPv3 and RMON 1 and 2, Third Edition; New Jersey, 1999

[37] US Army Signal Center, Specialized Training Branch. "Packet Switching" Student Guide, 4C-F55/260-F15/D03, Fort Gordon, 15 March 1996.